PCT/JP99/00292

日本国特許庁

22.02.99

PATENT OFFICE
JAPANESE GOVERNMENT

09/381996

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９８年　１月２６日

出願番号
Application Number: 平成１０年特許願第０１２４７４号

出願人
Applicant (s): 松下電器産業株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

１９９９年　３月２６日

特許庁長官
Commissioner,
Patent Office 伊佐山建志

出証番号　出証特平１１－３０１７３８８

【書類名】　特許願

【整理番号】　2054500002

【提出日】　平成10年 1月26日

【あて先】　特許庁長官殿

【国際特許分類】　G11B 20/10

【発明の名称】　データ記録再生方法およびデータ記録再生システム

【請求項の数】　38

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　山田　正純

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　飯塚　裕之

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　後藤　昌一

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　武知　秀明

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100092794

【弁理士】

【氏名又は名称】　松田　正道

【電話番号】　06 397-2840

【手数料の表示】

【予納台帳番号】　009896

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9006027

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ記録再生方法およびデータ記録再生システム

【特許請求の範囲】

【請求項１】　ディジタルデータにワークキーを用いて第１の暗号化を施した暗号化ディジタルデータと、前記ワークキーに第２の暗号化を施した暗号化ワークキーとを記録媒体に記録し、記録された前記暗号化ディジタルデータおよび前記暗号化ワークキーを再生し、前記暗号化ワークキーを解読して得られた前記ワークキーを用いて前記暗号化ディジタルデータを解読して、前記ディジタルデータを得ることを特徴とするデータ記録再生方法。

【請求項２】　前記暗号化ワークキーを、前記記録媒体の外部に出力されないデータ領域に記録することを特徴とする請求項１に記載のデータ記録再生方法。

【請求項３】　前記ワークキーを、定期的または不定期的に切り替えることを特徴とする請求項１または２に記載のデータ記録再生方法。

【請求項４】　外部からディジタルデータを受信する受信手段と、ワークキーを生成し、前記ディジタルデータに前記ワークキーを用いて第１の暗号化を施して暗号化ディジタルデータを生成する暗号化手段と、前記ワークキーに第２の暗号化を施して暗号化ワークキーを生成する鍵暗号化手段と、前記暗号化ディジタルデータおよび前記暗号化ワークキーを記録媒体に記録する記録手段と、前記記録媒体から前記暗号化ディジタルデータおよび前記暗号化ワークキーを再生する再生手段と、前記暗号化ワークキーを解読して前記ワークキーを復元する鍵復元手段と、復元された前記ワークキーを用いて前記暗号化ディジタルデータを解読して、前記ディジタルデータを得る暗号解読手段とを備えることを特徴とするデータ記録再生システム。

【請求項５】　前記全ての手段は、一体化された装置に備えられていることを特徴とする請求項４に記載のデータ記録再生システム。

【請求項６】　前記受信手段と、前記暗号化手段と、前記暗号解読手段とは、チューナ装置に備えられ、前記記録手段と、前記再生手段とは、ＶＴＲ装置に備えられていることを特徴とする請求項４に記載のデータ記録再生システム。

【請求項７】　前記第２の暗号化は、公開鍵を用いて施され、前記暗号化ワー

クキーの解読は、前記公開鍵に対応する秘密鍵を用いて施されることを特徴とする請求項６に記載のデータ記録再生システム。

【請求項８】　前記鍵復元手段は、前記チューナ装置に備えられていることを特徴とする請求項７に記載のデータ記録再生システム。

【請求項９】　前記公開鍵および前記秘密鍵は、前記チューナ装置に対して固有な鍵であることを特徴とする請求項８に記載のデータ記録再生システム。

【請求項１０】　前記公開鍵および前記秘密鍵は、前記チューナ装置の機器モデルに対して固有な鍵であることを特徴とする請求項８に記載のデータ記録再生システム。

【請求項１１】　前記チューナ装置は、ＩＣカードに記録された情報を読み取るカード読取手段を有することを特徴とする請求項８に記載のデータ記録再生システム。

【請求項１２】　前記公開鍵および前記秘密鍵は、前記ＩＣカードに記録されたユーザＩＤに対して固有な鍵であることを特徴とする請求項１１に記載のデータ記録再生システム。

【請求項１３】　前記ＩＣカードには、前記ユーザＩＤに対して固有な鍵に加えて、少なくとも一つの別のユーザＩＤに対して固有な公開鍵が記録されており、前記鍵暗号化手段は、前記第２の暗号化とともに、前記別のユーザＩＤに対して固有な公開鍵を用いて、前記ワークキーを暗号化して、前記別のユーザＩＤに対して固有な公開鍵毎に、別の暗号化ワークキーを生成し、前記記録手段は、前記暗号化ワークキーに加えて、前記別の暗号化ワークキーも前記記録媒体に記録することを特徴とする請求項１２に記載のデータ記録再生システム。

【請求項１４】　前記公開鍵および前記秘密鍵は、前記ＩＣカードに記録されたサービスに対して固有な鍵であることを特徴とする請求項１１に記載のデータ記録再生システム。

【請求項１５】　前記鍵暗号化手段は、前記チューナ装置または前記ＶＴＲ装置のいずれかに備えられていることを特徴とする請求項８～１４のいずれかに記載のデータ記録再生システム。

【請求項１６】　前記鍵暗号化手段が前記ＶＴＲ装置に備えられている場合は

、前記チューナ装置は、前記ワークキーを共通鍵によって暗号化する第二の鍵暗号化手段を有し、前記ＶＴＲ装置は、前記共通鍵によって暗号化された前記ワークキーを解読する第二の鍵復元手段を有することを特徴とする請求項１５に記載のデータ記録再生システム。

【請求項１７】　前記公開鍵および前記秘密鍵は、前記ＶＴＲ装置に対して固有な鍵であり、前記鍵暗号化手段および前記鍵復元手段は、前記ＶＴＲ装置に備えられていることを特徴とする請求項７に記載のデータ記録再生システム。

【請求項１８】　前記チューナ装置は、前記ワークキーを共通鍵によって暗号化する第二の鍵暗号化手段と、前記共通鍵によって暗号化された前記ワークキーを解読する第二の鍵復元手段とを有し、前記ＶＴＲ装置は、前記ワークキーを前記共通鍵によって暗号化する第三の鍵暗号化手段と、前記共通鍵によって暗号化された前記ワークキーを解読する第三の鍵復元手段とを有し、前記第三の鍵復元手段は、前記第二の鍵暗号化手段により暗号化された前記ワークキーを解読し、前記第二の鍵復元手段は、前記第三の鍵暗号化手段により暗号化された前記ワークキーを解読することを特徴とする請求項１７に記載のデータ記録再生システム。

【請求項１９】　前記第２の暗号化および前記暗号化ワークキーの解読は、共通鍵を用いて施され、前記鍵暗号化手段および前記鍵復元手段は、前記チューナ装置に備えられていることを特徴とする請求項６に記載のデータ記録再生システム。

【請求項２０】　前記共通鍵は、前記チューナ装置、もしくは、前記チューナ装置の機器モデルに対して固有な鍵であることを特徴とする請求項１９に記載のデータ記録再生システム。

【請求項２１】　前記チューナ装置は、ＩＣカードに記録された情報を読み取るカード読取手段を有し、前記共通鍵は、前記ＩＣカードに記録されたユーザＩＤ、もしくは、前記ＩＣカードに記録されたサービスに対して固有な鍵に対して固有な鍵であることを特徴とする請求項１９に記載のデータ記録再生システム。

【請求項２２】　前記チューナ装置は、前記記録媒体の記録時に課金情報を生成し、それを記憶することを特徴とする請求項６～２１のいずれかに記載のデー

タ記録再生システム。

【請求項２３】　前記チューナ装置は、前記記録媒体の再生時に課金情報を生成し、それを記憶することを特徴とする請求項６～２１のいずれかに記載のデータ記録再生システム。

【請求項２４】　前記記録媒体の記録時に、前記課金情報を生成するために必要な情報を、前記記録媒体に記録し、前記記録媒体の再生時に前記必要な情報を用いて前記課金情報を生成することを特徴とする請求項２３に記載のデータ記録再生システム。

【請求項２５】　前記課金情報は、前記記録媒体の再生期間の限定を伴うものであることを特徴とする請求項２３または２４に記載のデータ記録再生システム。

【請求項２６】　前記課金情報は、前記記録媒体の再生回数の限定を伴うものであることを特徴とする請求項２３～２５のいずれかに記載のデータ記録再生システム。

【請求項２７】　前記チューナ装置は、前記ＩＣカードに前記課金情報を記憶させることを特徴とする請求項２２～２６のいずれかに記載のデータ記録再生システム。

【請求項２８】　前記チューナ装置は、前記課金情報をサービスプロバイダに対して、通信を介して、出力することを特徴とする請求項２２～２７のいずれかに記載のデータ記録再生システム。

【請求項２９】　前記暗号化ワークキーを、前記記録媒体の外部に出力されないデータ領域に記録することを特徴とする請求項４～２８のいずれかに記載のデータ記録再生システム。

【請求項３０】　前記第２の暗号化を施した鍵の固有性に関する情報を、前記記録媒体に記録することを特徴とする請求項４～２９のいずれかに記載のデータ記録再生システム。

【請求項３１】　前記ワークキーを、定期的または不定期的に切り替えることを特徴とする請求項４～３０のいずれかに記載のデータ記録再生システム。

【請求項３２】　前記切り替えの後のワークキーに対応する前記暗号化ワーク

キーが、前記切り替えの前のワークキーに対応する前記暗号化ディジタルデータの少なくとも一部とタイミング的に重なるように、前記記録媒体は再生されることを特徴とする請求項３１に記載のデータ記録再生システム。

【請求項３３】　一つの前記ワークキーに対応する前記暗号化ワークキーが、それに対応する前記暗号化ディジタルデータとタイミング的に重なるように、前記記録媒体は再生されることを特徴とする請求項３１または３２に記載のデータ記録再生システム。

【請求項３４】　前記チューナ装置を備える場合は、前記チューナ装置が前記切り替えを行うことを特徴とする請求項３１～３３のいずれかに記載のデータ記録再生システム。

【請求項３５】　前記ＶＴＲ装置を備える場合は、前記ＶＴＲ装置が、前記切り替えに対応して、前記暗号化ワークキーの再生のタイミングを決定することを特徴とする請求項３１～３４のいずれかに記載のデータ記録再生システム。

【請求項３６】　前記暗号化ディジタルデータおよび前記暗号化ワークキーは、前記記録媒体上の前記再生のタイミングに対応する記録位置に、記録されることを特徴とする請求項３１～３５のいずれかに記載のデータ記録再生システム。

【請求項３７】　前記切り替えのタイミングも合わせて、前記記録媒体に記録することを特徴とする請求項３６に記載のデータ記録再生システム。

【請求項３８】　前記チューナ装置および前記ＶＴＲ装置を備える場合は、前記ＶＴＲ装置が、前記切り替えの後のワークキー、もしくは、それに対応する前記暗号化ワークキーを、前記切り替えの後のワークキーに対応する前記暗号化ディジタルデータの出力より前もって、前記チューナ装置へ出力することを特徴とする請求項３１～３７のいずれかに記載のデータ記録再生システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、データ記録再生方法およびデータ記録再生システムに関するものである。

【０００２】

【従来の技術】

衛星放送の録画、再生をユーザーが自由に行えると、少数のユーザーを介して、不特定多数の者に、録画された番組が無制限に供給されることが可能になるため、この対策を講ずることは、プロバイダにとって必要不可欠なことである。

【０００３】

以下に、従来の衛星放送の記録再生方法を、図２６を参照して説明する。図２６は、従来の衛星放送のデータ記録再生システムを示す構成図である。本システムは、衛星からの電波を受信するアンテナ９０３、ＩＣカード９０２に記録された情報に基づいて、受信した電波をＡＶデータに変換するＳＴＢ（Ｓｅｔ　Ｔｏｐ　Ｂｏｘ；衛星放送受信機）９０１、前記ＡＶデータを映像出力するモニター９０４、前記ＡＶデータを記録媒体９０６に記録／再生するＶＴＲ装置９０５から構成されている。

【０００４】

まず、希望の番組を視聴する場合の手順について説明する。ユーザーが視聴希望の番組を選択すると、その番組の視聴料金に対応する視聴用課金情報が、ＩＣカード９０２に記録される。原則として各番組のＡＶデータには、スクランブルがかけられており、当該番組の視聴用課金情報が、ＩＣカード９０２に記録されている場合のみ、ＳＴＢ９０１がスクランブルを解除して、スクランブルがない状態でモニター９０４が映像出力する。ただし、ＳＴＢ９０１がスクランブルを解除しても、当該ＡＶデータにはコピー防止信号（マクロビジョン）がかかっているため、この状態で、記録媒体に記録しても、再生時の再生画像が乱れてしまう。

【０００５】

次に、希望の番組を録画／再生する場合の手順について説明する。ユーザーが録画希望の番組を選択すると、その番組の録画料金に対応する録画用課金情報が、ＩＣカード９０２に記録される。当該番組の録画用課金情報が、ＩＣカード９０２に記録されている場合のみ、ＳＴＢ９０１が前述したマクロビジョンを解除して、乱れのないＡＶデータをＶＴＲ装置９０５に出力し、ＶＴＲ装置９０５は、これを記録媒体９０６に記録する。記録されたＡＶデータは、マクロビジョン

がかかってないため、通常のＡＶデータと同様の再生方法で、映像出力が得られる。

【０００６】

以上の手順で、ＩＣカード９０２に記録された視聴用課金情報および録画用課金情報は、一定期間分が電話回線等によって、プロバイダに通知される。

【０００７】

なお、図２６では、ＳＴＢ装置とＶＴＲ装置が分離したタイプの衛星放送のデータ記録再生システムについて説明したが、各装置の機能を一つの装置に集約したタイプのものもある。

【０００８】

【発明が解決しようとする課題】

しかしながら、上述した記録再生方法では、一度課金されて記録された記録媒体は、以後の課金無しで、何回でも再生でき、また、当該記録媒体を複製することも容易に行えるという問題点がある。

【０００９】

上記問題点の対策として、ＡＶデータが記録された記録媒体に、当該ＡＶデータ記録時に使用したＳＴＢおよび／またはＶＴＲ装置のＩＤも記録しておき、ＩＤが異なる機器で再生しようとすると、再生できないようにするという方法が提案されている。しかし、ＩＤ識別機能を有しない機器を用いる場合は、ＩＤの一致に関わりなく再生が可能であるという課題がある。また、全ての機器がＩＤ識別機能を有するとの前提に立てば、機器固有のＩＤを用いているために、当該機器が修復不可能な故障・破損等によって、使用できなくなった場合には、当該記録媒体に記録されたＡＶデータは、再生が不可能になってしまうという課題がある。

【００１０】

本発明は、上述した従来のデータ記録再生方法の課題を考慮し、データに暗号化を施すことによって、特定の対象に対してのみ、再生が可能であり、前記暗号化に関する情報が外部に漏洩しにくいデータ記録再生方法およびデータ記録再生システムを提供することを第一の目的とするものである。また、前記第一の目的

に加え、記録および／または再生時に、確実に課金が可能なデータ記録再生方法およびデータ記録再生システムを提供することを目的とするものである。さらに、前記第一の目的に加え、再生時のロスタイムが少ないデータ記録再生システムを提供することを目的とするものである。

【００１１】

【課題を解決するための手段】

上述した課題を解決するために、請求項１の本発明は、ディジタルデータにワークキーを用いて第１の暗号化を施した暗号化ディジタルデータと、前記ワークキーに第２の暗号化を施した暗号化ワークキーとを記録媒体に記録し、記録された前記暗号化ディジタルデータおよび前記暗号化ワークキーを再生し、前記暗号化ワークキーを解読して得られた前記ワークキーを用いて前記暗号化ディジタルデータを解読して、前記ディジタルデータを得ることを特徴とするデータ記録再生方法である。

【００１２】

請求項４の本発明は、外部からディジタルデータを受信する受信手段と、ワークキーを生成し、前記ディジタルデータに前記ワークキーを用いて第１の暗号化を施して暗号化ディジタルデータを生成する暗号化手段と、前記ワークキーに第２の暗号化を施して暗号化ワークキーを生成する鍵暗号化手段と、前記暗号化ディジタルデータおよび前記暗号化ワークキーを記録媒体に記録する記録手段と、前記記録媒体から前記暗号化ディジタルデータおよび前記暗号化ワークキーを再生する再生手段と、前記暗号化ワークキーを解読して前記ワークキーを復元する鍵復元手段と、復元された前記ワークキーを用いて前記暗号化ディジタルデータを解読して、前記ディジタルデータを得る暗号解読手段とを備えることを特徴とするデータ記録再生システムである。

【００１３】

請求項２２の本発明は、前記チューナ装置は、前記記録媒体の記録時に課金情報を生成し、それを記憶することを特徴とする請求項６～２１のいずれかに記載のデータ記録再生システムである。

【００１４】

請求項２３の本発明は、前記チューナ装置は、前記記録媒体の再生時に課金情報を生成し、それを記憶することを特徴とする請求項６～２１のいずれかに記載のデータ記録再生システムである。

【００１５】

請求項３０の本発明は、前記第２の暗号化を施した鍵の固有性に関する情報を、前記記録媒体に記録することを特徴とする請求項４～２９のいずれかに記載のデータ記録再生システムである。

【００１６】

【発明の実施の形態】

以下に、本発明の実施の形態を図面を参照して説明する。

【００１７】

（第１の実施の形態）

以下に、本発明の第１の実施の形態を図面を参照して説明する。

【００１８】

図１は、本発明の第１の実施の形態におけるデータ記録再生システムの構成を示す構成図である。本実施の形態におけるデータ記録再生システムは、本発明のチューナ装置に対応するＳＴＢ（Ｓｅｔ　Ｔｏｐ　Ｂｏｘ；衛星放送受信機）１と、ＳＴＢ１にユーザーＩＤ等の情報を与えるＩＣカード２と、ＳＴＢ１に接続されているアンテナ３およびモニター４と、本発明のＶＴＲ装置に対応するＶＴＲ装置５と、ＶＴＲ装置５によってデータを記録／再生される記録媒体６とから構成されている。

【００１９】

ＳＴＢ１は、ＩＣカード２に記録された情報の読み取り、必要情報をＩＣカード２に記録するカード読取手段１０と、ＳＴＢ１の機器ＩＤ等の情報を記憶するＳＴＢ情報記憶手段１１と、モニター４での出力画像に対してデコードされたＡＶデータを出力するデコーダ１２と、ワークキーを生成し、ＡＶデータに前記ワークキーを用いて暗号化を施して暗号化ＡＶデータを生成する暗号化手段１３と、前記ワークキーに第２の暗号化を施して暗号化ワークキーを生成する鍵暗号化手段１５と、前記暗号化ワークキーを解読して前記ワークキーを復元する鍵復元

手段１６と、復元された前記ワークキーを用いて前記暗号化ＡＶデータを解読して、前記ＡＶデータを得る暗号解読手段１４と、ＶＴＲ装置５とのデータの伝達を行うＶＴＲ伝達手段１７と、人工衛星からの電波をアンテナ３を介して受信して、ＳＴＢ１内部用の信号に変換する受信手段２０とを備えている。また、ＶＴＲ伝達手段１７は、ＶＴＲ装置５のＳＴＢ伝達手段５０と直接データの伝達を行うＤ－Ｉ／Ｆ（ディジタルインターフェイス）１８およびＶＴＲ装置５のＳＴＢ伝達手段５０と認証鍵の交換を行ってＶＴＲ装置５の確認を行う認証鍵交換部１９を有しており、受信手段２０は、アンテナ３と直結し、受信したデータの復調を行う受信復調部２１と、受信したデータに施されている放送用暗号を解除する放送用暗号解除部２２と、多重化されている受信データを分離するＤＭＵＸ（Ｄｅ－ｍｕｌｔｉｐｌｅｘｅｒ；分離部）２３とを有している。なお、ＳＴＢ１は、上記の他に、ＳＴＢ１の装置全体を制御するＳＴＢ制御手段（図示せず）を備えている。

【００２０】

ＶＴＲ装置５は、ＳＴＢ１とのデータの伝達を行うＳＴＢ伝達手段５０と、前記暗号化ＡＶデータおよび前記暗号化ワークキーを記録媒体６に記録する記録手段５３と、記録媒体６から前記暗号化ＡＶデータおよび前記暗号化ワークキーを再生する再生手段５６とを備えている。また、ＳＴＢ伝達手段５０は、ＳＴＢ１のＶＴＲ伝達手段１７と直接データの伝達を行うＤ－Ｉ／Ｆ（ディジタルインターフェイス）５１およびＳＴＢ１のＶＴＲ伝達手段１７と認証鍵の交換を行ってＳＴＢ１の確認を行う認証鍵交換部５２を有している。また、記録手段５３は、前記暗号化ＡＶデータおよび前記暗号化ワークキーに対して記録媒体６のフォーマットに適合した多重化を行うＭＵＸ（Ｍｕｌｔｉｐｌｅｘｅｒ；多重化部）５４および多重化されたデータを記録媒体６に記録する記録処理部５５を有しており、再生手段５６は、記録媒体６に記録されたデータを再生する再生処理部５８および多重化された再生データを分離するＤＭＵＸ（Ｄｅ－ｍｕｌｔｉｐｌｅｘｅｒ；分離部）５７とを有している。なお、ＶＴＲ装置５は、上記の他に、ＶＴＲ装置５の装置全体を制御するＶＴＲ制御手段（図示せず）を備えている。

【００２１】

次に、このような本実施の形態の動作を説明する。

【００２２】

まず、ＡＶデータを記録媒体６に記録する時のデータの流れを図２を用いて説明する。図２は、本発明の第１の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。図２において、図１で示した構成のうち、記録時に不要な手段等は、適宜省略して示す。また、Ｄは、記録しようとするＡＶデータの生データを、Ｋｗは、ＡＶデータＤの暗号化に用いるワークキーを、Ｋｗ（Ｄ）は、ＡＶデータＤにワークキーＫｗを用いて暗号化を施して得られる暗号化ＡＶデータを、$_{STB}$Ｐａは、ワークキーＫｗの暗号化に用いるＳＴＢ１に固有の公開鍵を、$_{STB}$Ｐａ（Ｋｗ）は、ワークキーＫｗに公開鍵$_{STB}$Ｐａを用いて暗号化を施して得られる暗号化ワークキーを、それぞれ示す。なお、本実施の形態におけるデータ記録再生システムは、ワークキーＫｗを、定期的または不定期的に切り替えることによって、切り替えない場合に比して、さらに、暗号化に関する情報が外部に漏洩しにくいシステムとなっている。

【００２３】

放送用電波として暗号化され、多重化されたＡＶデータＤは、アンテナ３を介して受信され、受信復調部２１で復調され、放送用の暗号を放送用暗号解除部２２で解除され、ＤＭＵＸ２３で分離されて、生のＡＶデータＤとなって、デコーダ１２および暗号化手段１３へ送られる。デコーダ１２は、ＡＶデータＤに施された高能率符号化処理等をデコードし、モニター４へ出力する。暗号化手段１３は、ワークキーＫｗを生成し、生成したワークキーＫｗを用いて、ＡＶデータＤに暗号化を施して、暗号化ＡＶデータＫｗ（Ｄ）を生成する。生成されたワークキーＫｗは、鍵暗号化手段１５へ送られ、鍵暗号化手段１５は、ＳＴＢ情報記憶手段１１に記憶されているＳＴＢ１に固有の公開鍵$_{STB}$Ｐａを用いて、ワークキーＫｗに暗号化を施して、暗号化ワークキー$_{STB}$Ｐａ（Ｋｗ）を生成する。

【００２４】

暗号化ＡＶデータＫｗ（Ｄ）は、Ｄ－Ｉ／Ｆ１８を介して、暗号化ワークキー$_{STB}$Ｐａ（Ｋｗ）は、認証鍵交換部１９およびＤ－Ｉ／Ｆ１８を介して、それぞれＶＴＲ装置５へ伝達されるが、それに先だって、ＳＴＢ１、ＶＴＲ装置５それ

ぞれの認証鍵交換部１９、５２は、Ｄ－Ｉ／Ｆ１８および５１を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

【００２５】

ＶＴＲ装置５へ伝達された暗号化ＡＶデータＫｗ（Ｄ）は、Ｄ－Ｉ／Ｆ５１を介して、暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ）は、Ｄ－Ｉ／Ｆ５１および認証鍵交換部５２を介して、それぞれＭＵＸ５４へ送られて、記録媒体６のフォーマットに適合した多重化を行われた後、記録処理部５５によって、記録媒体６に記録される。

【００２６】

次に、記録媒体６に記録されたＡＶデータを再生する時のデータの流れを図３を用いて説明する。図３は、本発明の第１の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図３において、図１で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。 $_{STB}$Ｓａは、公開鍵 $_{STB}$Ｐａに対応し、暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ）を解読してワークキーＫｗを復元するのに用いるＳＴＢ１に固有の秘密鍵を示す。図中の他の記号は、図２に倣う。

【００２７】

多重化されて記録媒体６に記録された暗号化ＡＶデータＫｗ（Ｄ）および暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ）は、再生処理部５８により再生され、ＤＭＵＸ５７で分離される。

【００２８】

分離された暗号化ＡＶデータＫｗ（Ｄ）は、Ｄ－Ｉ／Ｆ５１を介して、分離された暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ）は、認証鍵交換部５２およびＤ－Ｉ／Ｆ５１を介して、それぞれＳＴＢ１へ伝達されるが、それに先だって、記録時と同様に、ＳＴＢ１、ＶＴＲ装置５それぞれの認証鍵交換部１９、５２は、Ｄ－Ｉ／Ｆ１８および５１を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

【００２９】

ＳＴＢ１へ伝達された暗号化ＡＶデータＫｗ（Ｄ）は、Ｄ－Ｉ／Ｆ１８を介して、暗号解読手段１４へ送られ、暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ）は、Ｄ－Ｉ／Ｆ１８および認証鍵交換部１９を介して、鍵復元手段１６へ送られる。鍵復元手段１６は、ＳＴＢ情報記憶手段１１に記憶されているＳＴＢ１に固有の秘密鍵 $_{STB}$Ｓａを用いて、暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ）をワークキーＫｗに復元して、暗号解読手段１４へ送る。暗号解読手段１４は、復元されたワークキーＫｗを用いて、暗号化ＡＶデータＫｗ（Ｄ）を解読して得られるＡＶデータＤを、デコーダ１２へ出力する。デコーダ１２は、ＡＶデータＤに施された高能率符号化処理等をデコードし、モニター４へ出力する。

【００３０】

以上の手順にしたがって、ＡＶデータを記録／再生することにより、ＡＶデータに暗号化を施すのに用いたワークキーにＳＴＢ１に固有の公開鍵を用いて暗号化を施して、暗号化されたＡＶデータと一緒に記録媒体に記録し、再生時には暗号化されたワークキーをＳＴＢ１に固有の秘密鍵を用いて復元しているため、ＳＴＢ１に固有の秘密鍵を持っているシステム、すなわち、ＳＴＢ１そのものを備えているシステムしか再生できないので、本実施の形態におけるデータ記録再生システムは、特定の対象に対してのみ、再生が可能であり、暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムであることがわかる。

【００３１】

次に、本実施の形態におけるデータ記録再生システムの課金方法について説明する。本課金方法は、ＡＶデータの記録／再生時に課金するものであるため、図２、図３を参照して説明する。

【００３２】

まず、記録時の課金方法について説明する。図２において、ＳＴＢ１のＳＴＢ制御手段（図示せず）は、記録時に、課金情報を生成し、これをカード読取手段１０を介して、ＩＣカード２に記録させる。記録のタイミングとしては、例えば、ユーザーからの記録指令に連動して記録するとしてもよいし、暗号化手段１３または鍵暗号化手段１５の最初の出力に連動して記録するとしてもよい。記録する課金情報の内容としては、課金の金額そのものを記録するものであってもよい

し、課金内容を特定するための識別子のようなものであってもよい。

【００３３】

次に、再生時の課金方法について説明する。図３において、ＳＴＢ１のＳＴＢ制御手段（図示せず）は、再生時に、課金情報を生成し、これをカード読取手段１０を介して、ＩＣカード２に記録する。記録のタイミングとしては、例えば、ユーザーからの再生指令に連動して記録するとしてもよいし、暗号解読手段１４または鍵復元手段１６の最初の出力に連動して記録するとしてもよい。記録する課金情報の内容については、記録時と同様である。

【００３４】

ＩＣカード２に記録された課金情報は、定期的または不定期に、衛星放送のサービスプロバイダに対して、電話回線等の通信を介して出力され、サービスプロバイダは、この課金情報に基づいて、ユーザーの銀行口座からの引き落とし等の方法によって、ユーザーから課金の徴収を行う。

【００３５】

なお、上記説明において、課金情報は記録時および再生時に記録する、すなわち、記録、再生の両方に対して課金を行うとして説明したが、これに限らず、いずれか一方についてのみ、課金を行うとしてもよい。

【００３６】

また、課金情報は、カード読取手段１０を介して、ＩＣカード２に記録されるとして説明したが、これに限らず、例えば、ＳＴＢ情報記憶手段１１に記録されるとしてもよい。なお、ＳＴＢ情報記憶手段１１に記録される場合は、本実施の形態の構成におけるデータ記録再生システムから、ＩＣカード２およびカード読取手段１０を省いてもよい。

【００３７】

また、再生時の課金情報は、再生期間の限定および／または再生回数の限定を伴っていてもよい。例えば、ある期間を過ぎる、またはある再生回数を超えると、課金の金額が変わるというものでもよい。ただし、再生回数の限定を伴う場合には、再生する毎に、記録媒体６等に通算再生回数を示す情報を書き込む必要がある。

【００３８】

さらに、記録時に、再生時の課金情報を生成するために必要な情報を、記録媒体６に記録し、記録媒体６の再生時に前記必要な情報を用いて課金情報を生成するとしてもよい。このときは、例えば、ＳＴＢ制御手段が記録時に前記必要な情報を生成し、これを、ＶＴＲ伝達手段１７およびＳＴＢ伝達手段５０を介して、記録手段５３に送り、記録手段５３は、記録データの最初にこれを記録する。再生時には、前記必要な情報は、再生手段５６によって再生され、ＳＴＢ伝達手段５０およびＶＴＲ伝達手段１７を介して、ＳＴＢ制御手段へ送られ、ＳＴＢ制御手段は、これに基づいて、再生時の課金情報を生成する。

【００３９】

以上説明したところから、本実施の形態におけるデータ記録再生システムは、記録および／または再生時に、確実に課金が可能なデータ記録再生システムであることがわかる。

【００４０】

次に、本実施の形態におけるデータ記録再生システムによって、記録媒体に記録されるデータの、記録媒体上の記録領域について、図２、図４を参照して説明する。

【００４１】

図４は、本発明の第１の実施の形態におけるデータ記録再生システムを用いて記録された記録媒体上の記録領域を示す模式図である。図４の左右方向は、記録媒体６の時間的な記録位置を示し、上下方向は、同時刻に記録されたデータの構成を示す。図４において、記録領域は、メインエリアとサブエリアとに分けられており、メインエリアには、暗号化ＡＶデータと、ワークキー変更のタイミングを示すフラッグとが書き込まれており、サブエリアには、当該記録位置に対応するメインエリアの位置に記録された暗号化ＡＶデータ（Ｋｗ－ａ（Ｄ）、Ｋｗ－ｂ（Ｄ）、Ｋｗ－ｃ（Ｄ）、Ｋｗ－ｄ（Ｄ）、．．．）の暗号化に用いられたワークキー（Ｋｗ－ａ、Ｋｗ－ｂ、Ｋｗ－ｃ、Ｋｗ－ｄ、．．．）に、公開鍵 $_{STB}$Ｐａを用いて暗号化を施して得られた、暗号化ワークキー（ $_{STB}$Ｐａ（Ｋｗ－ａ）、 $_{STB}$Ｐａ（Ｋｗ－ｂ）、 $_{STB}$Ｐａ（Ｋｗ－ｃ）、 $_{STB}$Ｐａ（Ｋｗ－ｄ）、．

．．）と、次のワークキーの切替後のに用いられるワークキー（Ｋｗ－ｂ、Ｋｗ－ｃ、Ｋｗ－ｄ、Ｋｗ－ｅ、．．．）に、公開鍵 $_{STB}$Ｐａを用いて暗号化を施して得られた、暗号化ワークキー（ $_{STB}$Ｐａ（Ｋｗ－ｂ）、 $_{STB}$Ｐａ（Ｋｗ－ｃ）、 $_{STB}$Ｐａ（Ｋｗ－ｄ）、 $_{STB}$Ｐａ（Ｋｗ－ｅ）、．．．）とが書き込まれている。ただし、図４中においては、暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ－ａ）、 $_{STB}$Ｐａ（Ｋｗ－ｂ）、 $_{STB}$Ｐａ（Ｋｗ－ｃ）、 $_{STB}$Ｐａ（Ｋｗ－ｄ）、．．．は、便宜上、暗号化前のワークキーＫｗ－ａ、Ｋｗ－ｂ、Ｋｗ－ｃ、Ｋｗ－ｄ、．．．で表現している。

【００４２】

前述したように、暗号化手段１３は、ワークキーＫｗを定期的または不定期的に切り替えて生成し、生成したワークキーＫｗを用いて、ＡＶデータＤに暗号化を施して、暗号化ＡＶデータＫｗ（Ｄ）を生成するが、現在使用中のワークキー（例えば、Ｋｗ－ａ）の次の切替後のワークキー（例えば、Ｋｗ－ｂ）をあらかじめ生成して、その使用に先立って、鍵暗号化手段１５により暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ－ａ）に変換して、認証鍵交換部１９、Ｄ－Ｉ／Ｆ１８、５１を介して、ＭＵＸ５４へ送り、記録処理部５５は、これを現在使用中のワークキーＫｗ－ａ、それによって暗号化された暗号化ＡＶデータＫｗ－ａ（Ｄ）等とともに、図４に示した記録領域に記録する。なお、ワークキー変更のタイミングを示すフラッグは、例えば、ＡＶデータを伝送するパケットヘッダに付加されて伝達されてくるものとし、記録処理部５５は、これをもとに、各記録データの記録位置を決定する。

【００４３】

図４に示すように、切り替えの後のワークキー、例えば、Ｋｗ－ｂ、に対応する暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ－ｂ）は、切り替えの前のワークキーＫｗ－ａに対応する暗号化ＡＶデータＫｗ－ａ（Ｄ）の少なくとも一部と重なるように、記録媒体６に記録されており、切り替えの前のワークキーＫｗ－ａは、それに対応する暗号化ＡＶデータＫｗ－ａ（Ｄ）が記録されている位置に重なって、記録媒体６に記録されている。なお、暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ－ｂ）の記録領域は、図４においては、その次のワークキーＫｗ－ｃに対応する暗号化ワー

クキー $_{STB}$Ｐａ（Ｋｗ－ｃ）が書き込まれる直前まで書き込まれているが、少なくとも暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ－ｃ）が書き込まれる前に書き込みが終了していればよい、すなわち、図４中の暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ－ｂ）の記録領域は、少なくとも暗号化ＡＶデータＫｗ－ａ（Ｄ）の一部と重なるように記録されておれば、暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ－ｃ）の記録領域の始端との間にデータの空白領域があってもよい。

【００４４】

以上の記録要領によって、記録媒体への記録を行うことによって、再生時には、次のワークキーをあらかじめ解読できるので、本実施の形態におけるデータ記録再生システムは、再生時のロスタイムが少ないデータ記録再生システムであることがわかる。

【００４５】

なお、本発明の記録媒体上の記録領域への記録要領は、本実施の形態における上述した記録要領に限るものではなく、例えば、暗号化手段１３が次の切替後のワークキーをあらかじめ生成せず、ＶＴＲ装置５が、ＳＴＢ１から送られてくるデータを一時記憶する手段を有し、前記一時記憶する手段に現在のデータを一時記憶させて、ワークキー切替後のデータを受け取った後に、記録媒体６への記録領域を決定して、記録するとしてもよい。

【００４６】

また、上述した記録要領に加えて、ワークキーＫｗの暗号化に用いた鍵を特定できる情報を記録媒体６に記録するとしてもよい。具体的には、本実施の形態においては、ＳＴＢ１のＩＤ情報である。この情報を利用して、例えば、ＳＴＢ１以外のＳＴＢを用いて再生をしようとした場合、当該ＳＴＢでは再生できない旨の警告とともに、再生可能なＳＴＢ（ここではＳＴＢ１）のＩＤ情報を表示することができる。

【００４７】

また、暗号化ワークキーを記録媒体６中の外部に出力されないデータ領域に記録してもよい。例えば、Ｄ－ＶＨＳシステムであれば、サブコード領域に記録する。これによって、さらに、暗号化に関する情報が外部に漏洩しにくいデータ記

録再生システムとなる。

【００４８】

さらに、本実施の形態においては、暗号化ディジタルデータおよび暗号化ワークキーは、記録媒体上の再生のタイミングに対応する記録位置に記録されるとして説明したが、これに限るものではなく、記録位置にとらわれず、切り替えの後のワークキーに対応する暗号化ワークキーが、切り替えの前のワークキーに対応する暗号化ディジタルデータの少なくとも一部とタイミング的に重なるように、また、一つのワークキーに対応する暗号化ワークキーが、それに対応する暗号化ディジタルデータとタイミング的に重なるように、再生されさえすればよい。

【００４９】

なお、上述した本実施の形態の課金方法および／または記録媒体上の記録領域への記録要領の替わりに、従来のものを用いる場合においては、上述したそれぞれの効果は得られないものの、特定の対象に対してのみ、再生が可能であり、暗号化に関する情報が外部に漏洩しにくいデータ記録再生方法およびデータ記録再生システムを提供するという、本発明の第一の目的は満足するものである。

【００５０】

（第２の実施の形態）

以下に、本発明の第２の実施の形態を図面を参照して説明する。本実施の形態が上述した第１の実施の形態と異なる点は、ワークキーの暗号化／復元を行う公開鍵／秘密鍵が、本発明のチューナ装置の機器モデルに対して固有な鍵であることに関する点である。したがって、本実施の形態において、第１の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第１の実施の形態と同じとする。

【００５１】

本実施の形態におけるデータ記録再生システムの構成は、第１の実施の形態におけるデータ記録再生システムの構成と同じである。

【００５２】

次に、このような本実施の形態の動作を説明する。

【００５３】

本実施の形態においては、ワークキーＫｗの暗号化にＳＴＢ１の機器モデルに固有の公開鍵$_{STBU}$Ｐａを用い、ワークキーＫｗを復元するのにＳＴＢ１の機器モデルに固有の秘密鍵$_{STBU}$Ｓａを用いている点以外は、第１の実施の形態におけるデータ記録再生システムと同じである。したがって、本実施の形態の動作は、図２、図３において、公開鍵$_{STB}$Ｐａ、秘密鍵$_{STB}$Ｓａおよび暗号化ワークキー$_{STB}$Ｐａ（Ｋｗ）を、それぞれ、公開鍵$_{STBU}$Ｐａ、秘密鍵$_{STBU}$Ｓａおよび暗号化ワークキー$_{STBU}$Ｐａ（Ｋｗ）に置き換えたもので示されるので、詳細の説明は、図２、図３に倣うとして省略する。

【００５４】

以上の手順にしたがって、ＡＶデータを記録／再生することにより、本実施の形態は、第１の実施の形態によって得られる効果に加え、図５に示すように、ＳＴＢ１と同じモデルであるＳＴＢ１０１を所有しているユーザー間での記録媒体６の貸し借りが可能となり、かつ、ＳＴＢ１が修復不可能な故障・破損等によって、使用できなくなった場合においても、同じ機器モデルのＳＴＢに代替すれば、引き続き使用できるものであることがわかる。

【００５５】

（第３の実施の形態）

以下に、本発明の第３の実施の形態を図面を参照して説明する。本実施の形態が上述した第１の実施の形態と異なる点は、ワークキーの暗号化／復元を行う公開鍵／秘密鍵が、本発明のＩＣカードに記録されたユーザＩＤに対して固有な鍵であることに関する点である。したがって、本実施の形態において、第１の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第１の実施の形態と同じとする。

【００５６】

本実施の形態におけるデータ記録再生システムの構成は、第１の実施の形態におけるデータ記録再生システムの構成と同じである。

【００５７】

次に、このような本実施の形態の動作を説明する。

図６は、本発明の第２の実施の形態におけるデータ記録再生システムのデータ

記録時のデータの流れを示すフロー図であり、図７は、本発明の第２の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図６、図７に示すとおり、本実施の形態においては、ワークキーＫｗの暗号化にＩＣカード２に記録されたユーザＩＤに対して固有の公開鍵$_{USER}$Ｐａを用い、ワークキーＫｗを復元するのにユーザＩＤに対して固有の秘密鍵$_{USER}$Ｓａを用いている点以外は、第１の実施の形態におけるデータ記録再生システムと同じである。

【００５８】

以上の手順にしたがって、ＡＶデータを記録／再生することにより、本実施の形態は、第１の実施の形態によって得られる効果に加え、ＳＴＢ１が修復不可能な故障・破損等によって、使用できなくなった場合においても、他のＳＴＢ（同じ機器モデルでなくても可）に代替すれば、引き続き使用でき、かつ、ＩＣカード２と一緒に記録媒体６の貸し借りをすれば、他のユーザーの使用が可能となるものであることがわかる。

【００５９】

また、本実施の形態において、上述のようにワークキーＫｗの暗号化にＩＣカード２に記録されたユーザＩＤに対して固有の公開鍵$_{USER}$Ｐａを用いて、暗号化ワークキー$_{USER}$Ｐａ（Ｋｗ）を生成するとともに、同じくＩＣカード２に記録された他のユーザＩＤに対して固有の公開鍵$_{USER1}$Ｐａを用いて、暗号化ワークキー$_{USER1}$Ｐａ（Ｋｗ）も生成して、暗号化ワークキー$_{USER}$Ｐａ（Ｋｗ）とともに、記録媒体６に記録しておけば、ＩＣカード２を貸し出さなくても、公開鍵$_{USER1}$Ｐａに対応する秘密鍵$_{USER1}$Ｓａを保持している特定のユーザーは、その$_{USER1}$Ｓａを用いて暗号化ワークキー$_{USER1}$Ｐａ（Ｋｗ）を復元できるので、その特定のユーザーに対してのみ、記録媒体６の貸し出し使用が可能となる。なお、公開鍵$_{USER1}$Ｐａは、単数に限るものではなく、公開鍵$_{USER1}$Ｐａ～$_{USERn}$Ｐａと、複数個であってもよい。すなわち、ユーザーは、貸し出し使用をしたい他のユーザーが生じた場合には、所定の手続を経て、ＩＣカード２に、当該他のユーザーに対応する公開鍵$_{USERn}$Ｐａを記録して貰うことによって、当該他のユーザーへの簡単な貸し出し使用が可能となるものである。

【００６０】

なお、上記動作からわかるように、本実施の形態においては、図１に示した第１の実施の形態におけるデータ記録再生システムの構成から、ＳＴＢ記憶手段１１を省略したものであってもよい。

【００６１】

（第４の実施の形態）

以下に、本発明の第４の実施の形態を図面を参照して説明する。本実施の形態が上述した第１の実施の形態と異なる点は、ワークキーの暗号化／復元を行う公開鍵／秘密鍵が、本発明のＩＣカードに記録されたサービスに対して固有な鍵であることに関する点である。したがって、本実施の形態において、第１の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第１の実施の形態と同じとする。

【００６２】

本実施の形態におけるデータ記録再生システムの構成は、第１の実施の形態におけるデータ記録再生システムの構成と同じである。

【００６３】

次に、このような本実施の形態の動作を説明する。

【００６４】

図８は、本発明の第４の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図であり、図９は、本発明の第４の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図８、図９に示すとおり、本実施の形態においては、ワークキーＫｗの暗号化にＩＣカード２に記録されたサービスに対して固有の公開鍵$_{SERV}$Ｐａを用い、ワークキーＫｗを復元するのにＳＴＢ１の機器モデルに固有の秘密鍵$_{SERV}$Ｓａを用いている点以外は、第１の実施の形態におけるデータ記録再生システムと同じである。ここで、サービスに対して固有の鍵とは、具体的には、特定の番組に対してのみ固有、特定のジャンルの番組に対してのみ固有、特定のチャンネル番組に対してのみ固有、特定の衛星放送のプロバイダに対してのみ固有の鍵等が挙げられる。

【００６５】

例えば、特定の番組の記録／再生に対して、前もって料金を支払うことにより、その番組に固有の公開鍵$_{SERV}$Ｐａおよび秘密鍵$_{SERV}$ＳａをＩＣカード２に記憶させてもらうことにより、前記特定の番組の記録／再生が可能となるものである。この場合、公開鍵$_{SERV}$Ｐａおよび秘密鍵$_{SERV}$ＳａがＩＣカード２に記憶されていなければ、記録できなくなる措置をＳＴＢ１が有する必要がある。なお、公開鍵$_{SERV}$Ｐａおよび秘密鍵$_{SERV}$Ｓａが必要な特定の番組以外の番組に対しては、第１～第３の実施の形態のいずれかで用いた公開鍵および秘密鍵に切り替えて、これらを用いるという、併用も可能である。

【００６６】

以上の手順にしたがって、ＡＶデータを記録／再生することにより、本実施の形態は、第１の実施の形態によって得られる効果に加え、ＳＴＢ１が修復不可能な故障・破損等によって、使用できなくなった場合においても、他のＳＴＢ（同じ機器モデルでなくても可）に代替すれば、引き続き使用でき、かつ、記録されたＡＶデータに対応する特定のサービスを享受することを許可された特定のユーザーに対してのみ、記録媒体６の貸し借り使用が可能となるものであることがわかる。

【００６７】

なお、上記動作からわかるように、本実施の形態においては、図１に示した第１の実施の形態におけるデータ記録再生システムの構成から、ＳＴＢ記憶手段１１を省略したものであってもよい。

【００６８】

（第５の実施の形態）

以下に、本発明の第５の実施の形態を図面を参照して説明する。本実施の形態が上述した第１の実施の形態と異なる点は、本発明の鍵暗号化手段がＶＴＲ装置に備えられており、それに伴って、本発明のチューナ装置が、ワークキーを共通鍵によって暗号化する第二の鍵暗号化手段を有し、本発明のＶＴＲ装置が、前記共通鍵によって暗号化された前記ワークキーを解読する第二の鍵復元手段を有することに関する点である。したがって、本実施の形態において、第１の実施の形

態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第１の実施の形態と同じとする。

【００６９】

図１０は、本発明の第５の実施の形態におけるデータ記録再生システムの構成を示す構成図である。本実施の形態におけるデータ記録再生システムの構成が、第１の実施の形態におけるデータ記録再生システムの構成と異なるのは、本発明の鍵暗号化手段に対応する鍵暗号化手段６２が、ＳＴＢ１ではなく、ＶＴＲ装置５に備えられており、それに伴い、ＳＴＢ１は、本発明の第二の鍵暗号化手段対応する鍵暗号化手段３１を有し、ＶＴＲ装置５は、本発明の第二の鍵復元手段に対応する鍵復元手段６１と、鍵復元手段６１および鍵暗号化手段６２が用いる共通鍵、公開鍵等の情報を記憶するＶＴＲ情報記憶手段７１とを有している。また、ＳＴＢ情報記憶手段１１は、第１の実施の形態において保持していた情報に加えて、鍵暗号化手段３１がワークキーを暗号化するのに用いる共通鍵の情報を保持している。

【００７０】

なお、第１の実施の形態と同様に、課金情報が、例えば、ＳＴＢ情報記憶手段１１に記録される場合は、本実施の形態の構成におけるデータ記録再生システムから、ＩＣカード２およびカード読取手段１０を省いてもよい。

【００７１】

次に、このような本実施の形態の動作を説明する。

【００７２】

まず、ＡＶデータを記録媒体６に記録する時のデータの流れを図１１を用いて説明する。図１１は、本発明の第５の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。図１１において、図１０で示した構成のうち、記録時に不要な手段等は、適宜省略して示す。また、図中の記号については、新たに説明するもの以外は、図２、図３に倣う。Ｋｃは、ワークキーＫｗの暗号化に用いるＳＴＢ１およびＶＴＲ装置５に共通な共通鍵を、ＡＶデータＤの暗号化に用いるワークキーを、Ｋｃ（Ｋｗ）は、ワークキーＫｗに共通鍵Ｋｃを用いて暗号化を施して得られる暗号化ワークキーを、それぞれ

示す。なお、本実施の形態におけるデータ記録再生システムは、第１の実施の形態と同様に、ワークキーＫｗを、定期的または不定期的に切り替えることによって、切り替えない場合に比して、さらに、暗号化に関する情報が外部に漏洩しにくいシステムとなっている。

【００７３】

放送用電波として暗号化され、多重化されたＡＶデータＤは、アンテナ３を介して受信され、受信復調部２１で復調され、放送用の暗号を放送用暗号解除部２２で解除され、ＤＭＵＸ２３で分離されて、生のＡＶデータＤとなって、デコーダ１２および暗号化手段１３へ送られる。デコーダ１２は、ＡＶデータＤに施された高能率符号化処理等をデコードし、モニター４へ出力する。暗号化手段１３は、ワークキーＫｗを生成し、生成したワークキーＫｗを用いて、ＡＶデータＤに暗号化を施して、暗号化ＡＶデータＫｗ（Ｄ）を生成する。生成されたワークキーＫｗは、鍵暗号化手段３１へ送られ、鍵暗号化手段３１は、ＳＴＢ情報記憶手段１１に記憶されているＳＴＢ１およびＶＴＲ装置５に共通な共通鍵Ｋｃを用いて、ワークキーＫｗに暗号化を施して、暗号化ワークキーＫｃ（Ｋｗ）を生成する。

【００７４】

暗号化ＡＶデータＫｗ（Ｄ）は、Ｄ－Ｉ／Ｆ１８を介して、暗号化ワークキーＫｃ（Ｋｗ）は、認証鍵交換部１９およびＤ－Ｉ／Ｆ１８を介して、それぞれＶＴＲ装置５へ伝達されるが、それに先だって、ＳＴＢ１、ＶＴＲ装置５それぞれの認証鍵交換部１９、５２は、Ｄ－Ｉ／Ｆ１８および５１を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

【００７５】

ＶＴＲ装置５へ伝達された暗号化ＡＶデータＫｗ（Ｄ）は、Ｄ－Ｉ／Ｆ５１を介して、ＭＵＸ５４へ送られる。また、ＶＴＲ装置５へ伝達された暗号化ワークキーＫｃ（Ｋｗ）は、Ｄ－Ｉ／Ｆ５１および認証鍵交換部５２を介して、鍵復元手段６１に送られる。鍵復元手段６１は、ＶＴＲ情報記憶手段７１に記憶されている共通鍵Ｋｃを用いて、暗号化ワークキーＫｃ（Ｋｗ）をワークキーＫｗに復

元して、鍵暗号化手段６２に送る。鍵暗号化手段６２は、ＶＴＲ情報記憶手段７１に記憶されているＳＴＢ１に固有の公開鍵 $_{STB}$Ｐａを用いて、ワークキーＫｗに暗号化を施して、暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ）を生成して、これをＭＵＸ５４へ送る。ＭＵＸ５４へ送られた暗号化ＡＶデータＫｗ（Ｄ）および暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ）は、記録媒体６のフォーマットに適合した多重化を行われた後、記録処理部５５によって、記録媒体６に記録される。

【００７６】

次に、記録媒体６に記録されたＡＶデータを再生する時のデータの流れを図１２を用いて説明する。図１２は、本発明の第５の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図１２からわかるように、本実施の形態においては、記録された暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ）は、ＶＴＲ装置５内では復元されずに、ＳＴＢ１の鍵復元手段１６へ送られ、ここで、ＳＴＢ情報記憶手段１１に記憶されているＳＴＢ１に固有の秘密鍵 $_{STB}$Ｓａを用いることによって、ワークキーＫｗに復元される。図１で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。すなわち、ＡＶデータを再生する時のデータの流れは、第１の実施の形態の図３と同じになる。

【００７７】

以上の手順にしたがって、ＡＶデータを記録／再生することにより、ＡＶデータの記録時において、ＶＴＲ装置５への送信側であるＳＴＢ１におけるワークキーの暗号化が、負担の軽い共通鍵による暗号化としているので、ＡＶデータの暗号化およびワークキーの暗号化を平行しておこなうことにより負担が増大しているＳＴＢ１の負担を軽減できるので、本実施の形態におけるデータ記録再生システムは、特定の対象に対してのみ、再生が可能であり、暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムであり、かつ、第１の実施の形態におけるデータ記録再生システムと比較して、ＳＴＢ１およびＶＴＲ装置５の負担を平滑化して、記録効率の向上を図ることが可能なシステムであることがわかる。

【００７８】

なお、本発明の公開鍵および秘密鍵は、本実施の形態においては、第１の実施の形態と同じく、本発明のチューナ装置（ＳＴＢ１）に対して固有な鍵であると

して説明したが、これに限るものではなく、例えば、第２～第４いずれかの実施の形態と同じく、本発明のチューナ装置（ＳＴＢ１）の機器モデルに対して固有な鍵、本発明のＩＣカードに記録されたユーザＩＤに対して固有な鍵、本発明のＩＣカードに記録されたサービスに対して固有な鍵であってもよい。

【００７９】

また、本発明の公開鍵の情報は、本実施の形態においては、ＶＴＲ情報記憶手段７１に記憶されているものとして説明したが、これに限るものではなく、例えば、記録を始める際に、ＳＴＢ１から送られてくるとしてもよい。

【００８０】

なお、本実施の形態におけるデータ記録再生システムから、図１３に示すように、鍵暗号化手段３１および鍵復元手段６１を省略した構成も可能である。こうすれば、本発明のチューナ装置からＶＴＲ装置へのデータ送信において、ワークキーに暗号化を施さずに送信を行うことになる。このような構成は、後述する第８の実施の形態のように、ＳＴＢおよびＶＴＲ装置の機能を一体化した一体化ＳＴＢを備えるデータ記録再生システムに適用すると、特に有効である。以下に、図１３の構成のデータ記録再生システムについて説明する。

【００８１】

図１３の構成のデータ記録再生システムにおける、ＡＶデータを記録媒体６に記録する時のデータの流れは、図１４に示すようになる。図１４において、図１３で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。また、図中の記号については、図１１、図１２に倣う。

【００８２】

放送用電波として暗号化され、多重化されたＡＶデータＤは、アンテナ３を介して受信され、受信復調部２１で復調され、放送用の暗号を放送用暗号解除部２２で解除され、ＤＭＵＸ２３で分離されて、生のＡＶデータＤとなって、デコーダ１２および暗号化手段１３へ送られる。デコーダ１２は、ＡＶデータＤに施された高能率符号化処理等をデコードし、モニター４へ出力する。暗号化手段１３は、ワークキーＫｗを生成し、生成したワークキーＫｗを用いて、ＡＶデータＤに暗号化を施して、暗号化ＡＶデータＫｗ（Ｄ）を生成する。

【００８３】

暗号化ＡＶデータＫｗ（Ｄ）は、Ｄ－Ｉ／Ｆ１８を介して、ワークキーＫｗは、認証鍵交換部１９およびＤ－Ｉ／Ｆ１８を介して、それぞれＶＴＲ装置５へ伝達されるが、それに先だって、ＳＴＢ１、ＶＴＲ装置５それぞれの認証鍵交換部１９、５２は、Ｄ－Ｉ／Ｆ１８および５１を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

【００８４】

ＶＴＲ装置５へ伝達された暗号化ＡＶデータＫｗ（Ｄ）は、Ｄ－Ｉ／Ｆ５１を介して、ＭＵＸ５４へ送られる。また、ＶＴＲ装置５へ伝達されたワークキーＫｗは、Ｄ－Ｉ／Ｆ５１および認証鍵交換部５２を介して、鍵暗号化手段６２に送られる。鍵暗号化手段６２は、ＶＴＲ情報記憶手段７１に記憶されているＳＴＢ１に固有の公開鍵 $_{STB}$Ｐａを用いて、ワークキーＫｗに暗号化を施して、暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ）を生成して、これをＭＵＸ５４へ送る。ＭＵＸ５４へ送られた暗号化ＡＶデータＫｗ（Ｄ）および暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ）は、記録媒体６のフォーマットに適合した多重化を行われた後、記録処理部５５によって、記録媒体６に記録される。

【００８５】

図１３の構成のデータ記録再生システムにおける、データ再生時のデータの流れについては、図１２で示したデータ再生時のデータの流れと同じである。したがって、以下の説明を省略する。

【００８６】

なお、ＳＴＢ情報記憶手段１１およびＶＴＲ情報記憶手段７１は、図１０の構成において保持していた共通鍵の情報を保持している必要はない。

【００８７】

以上の手順にしたがって、ＡＶデータを記録／再生することにより、ＡＶデータの記録時において、ＶＴＲ装置５への送信側であるＳＴＢ１がワークキーの暗号化を行わないので、ＡＶデータの暗号化およびワークキーの暗号化を平行しておこなうことにより負担が増大しているＳＴＢ１の負担をさらに軽減できるので、図１３の構成のデータ記録再生システムは、図１０の構成のデータ記録再生シ

ステムと比較して、ＳＴＢ１およびＶＴＲ装置５の負担をさらに平滑化して、記録効率の向上を図ることが可能なシステムであることがわかる。ただし、図１０の構成のデータ記録再生システムと比較して、ＳＴＢ１からＶＴＲ装置５へのデータ送信についてのセキュリティは低下する。このような構成は、後述する第８の実施の形態のように、ＳＴＢおよびＶＴＲ装置の機能を一体化した一体化ＳＴＢを備えるデータ記録再生システムに適用すると、特に有効である。

【００８８】

（第６の実施の形態）

以下に、本発明の第６の実施の形態を図面を参照して説明する。本実施の形態が上述した第１の実施の形態と異なる点は、本発明の鍵暗号化手段および鍵復元手段がＶＴＲ装置に備えられており、ワークキーの暗号化／復元を行う公開鍵／秘密鍵が、本発明のＶＴＲ装置に対して固有な鍵であることに関する点である。したがって、本実施の形態において、第１の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第１の実施の形態と同じとする。

【００８９】

図１５は、本発明の第６の実施の形態におけるデータ記録再生システムの構成を示す構成図である。本実施の形態におけるデータ記録再生システムの構成が、第１の実施の形態におけるデータ記録再生システムの構成と異なるのは、本発明の鍵暗号化手段に対応する鍵暗号化手段６２および本発明の鍵復元手段に対応する鍵復元手段６４が、ＳＴＢ１ではなく、ＶＴＲ装置５に備えられており、それに伴い、ＳＴＢ１は、本発明の第二の鍵暗号化手段に対応する鍵暗号化手段３１および本発明の第二の鍵復元手段に対応する鍵復元手段３２を有し、ＶＴＲ装置５は、本発明の第二の鍵復元手段に対応する鍵復元手段６１と、本発明の第二の鍵暗号化手段に対応する鍵暗号化手段６３と、鍵復元手段６１、鍵暗号化手段６２、鍵暗号化手段６３および鍵復元手段６４が用いる共通鍵、公開鍵等の情報を記憶するＶＴＲ情報記憶手段７１とを有している。また、ＳＴＢ情報記憶手段１１は、第１の実施の形態において保持していた情報に加えて、鍵暗号化手段３１がワークキーを暗号化するのに用いる共通鍵の情報を保持している。

【００９０】

なお、第１の実施の形態と同様に、課金情報が、例えば、ＳＴＢ情報記憶手段１１に記録される場合は、本実施の形態の構成におけるデータ記録再生システムから、ＩＣカード２およびカード読取手段１０を省いてもよい。

【００９１】

次に、このような本実施の形態の動作を説明する。

【００９２】

まず、ＡＶデータを記録媒体６に記録する時のデータの流れを図１４を用いて説明する。図１６は、本発明の第６の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。図１６において、図１５で示した構成のうち、記録時に不要な手段等は、適宜省略して示す。また、図中の記号については、新たに説明するもの以外は、図２、図３に倣う。Ｋｃは、ワークキーＫｗの暗号化に用いるＳＴＢ１およびＶＴＲ装置５に共通な共通鍵を、Ｋｃ（Ｋｗ）は、ワークキーＫｗに共通鍵Ｋｃを用いて暗号化を施して得られる暗号化ワークキーを、$_{VTR}$Ｐａは、ワークキーＫｗの暗号化に用いるＶＴＲ装置５に固有の公開鍵を、$_{VTR}$Ｐａ（Ｋｗ）は、ワークキーＫｗに公開鍵$_{VTR}$Ｐａを用いて暗号化を施して得られる暗号化ワークキーを、それぞれ示す。なお、本実施の形態におけるデータ記録再生システムは、第１の実施の形態と同様に、ワークキーＫｗを、定期的または不定期的に切り替えることによって、切り替えない場合に比して、さらに、暗号化に関する情報が外部に漏洩しにくいシステムとなっている。

【００９３】

放送用電波として暗号化され、多重化されたＡＶデータＤは、アンテナ３を介して受信され、受信復調部２１で復調され、放送用の暗号を放送用暗号解除部２２で解除され、ＤＭＵＸ２３で分離されて、生のＡＶデータＤとなって、デコーダ１２および暗号化手段１３へ送られる。デコーダ１２は、ＡＶデータＤに施された高能率符号化処理等をデコードし、モニター４へ出力する。暗号化手段１３は、ワークキーＫｗを生成し、生成したワークキーＫｗを用いて、ＡＶデータＤに暗号化を施して、暗号化ＡＶデータＫｗ（Ｄ）を生成する。生成されたワーク

キーＫｗは、鍵暗号化手段３１へ送られ、鍵暗号化手段３１は、ＳＴＢ情報記憶手段１１に記憶されているＳＴＢ１およびＶＴＲ装置５に共通な共通鍵Ｋｃを用いて、ワークキーＫｗに暗号化を施して、暗号化ワークキーＫｃ（Ｋｗ）を生成する。

【００９４】

暗号化ＡＶデータＫｗ（Ｄ）は、Ｄ－Ｉ／Ｆ１８を介して、暗号化ワークキー$_{STB}$Ｐａ（Ｋｗ）は、認証鍵交換部１９およびＤ－Ｉ／Ｆ１８を介して、それぞれＶＴＲ装置５へ伝達されるが、それに先だって、ＳＴＢ１、ＶＴＲ装置５それぞれの認証鍵交換部１９、５２は、Ｄ－Ｉ／Ｆ１８および５１を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

【００９５】

ＶＴＲ装置５へ伝達された暗号化ＡＶデータＫｗ（Ｄ）は、Ｄ－Ｉ／Ｆ５１を介して、ＭＵＸ５４へ送られる。また、ＶＴＲ装置５へ伝達された暗号化ワークキーＫｃ（Ｋｗ）は、Ｄ－Ｉ／Ｆ５１および認証鍵交換部５２を介して、鍵復元手段６１に送られる。鍵復元手段６１は、ＶＴＲ情報記憶手段７１に記憶されている共通鍵Ｋｃを用いて、暗号化ワークキーＫｃ（Ｋｗ）をワークキーＫｗに復元して、鍵暗号化手段６２に送る。鍵暗号化手段６２は、ＶＴＲ情報記憶手段７１に記憶されているＶＴＲ装置５に固有の公開鍵 $_{VTR}$Ｐａを用いて、ワークキーＫｗに暗号化を施して、暗号化ワークキー $_{VTR}$Ｐａ（Ｋｗ）を生成して、これをＭＵＸ５４へ送る。ＭＵＸ５４へ送られた暗号化ＡＶデータＫｗ（Ｄ）および暗号化ワークキー $_{VTR}$Ｐａ（Ｋｗ）は、記録媒体６のフォーマットに適合した多重化を行われた後、記録処理部５５によって、記録媒体６に記録される。

【００９６】

次に、記録媒体６に記録されたＡＶデータを再生する時のデータの流れを図１７を用いて説明する。図１７は、本発明の第６の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図１７において、図１５で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。 $_{VTR}$Ｓａは、公開鍵 $_{VTR}$Ｐａに対応し、暗号化ワークキー $_{VTR}$Ｐａ（Ｋｗ）を

解読してワークキーＫｗを復元するのに用いるＶＴＲ装置５に固有の秘密鍵を示す。図中の他の記号は、図１６に倣う。

【００９７】

多重化されて記録媒体６に記録された暗号化ＡＶデータＫｗ（Ｄ）および暗号化ワークキー $_{VTR}$Ｐａ（Ｋｗ）は、再生処理部５８により再生され、ＤＭＵＸ５７で分離される。分離された暗号化ワークキー $_{VTR}$Ｐａ（Ｋｗ）は、鍵復元手段６４へ送られる。鍵復元手段６４は、ＶＴＲ情報記憶手段７１に記憶されているＶＴＲ装置５に固有の秘密鍵 $_{VTR}$Ｓａを用いて、暗号化ワークキー $_{VTR}$Ｐａ（Ｋｗ）をワークキーＫｗに復元して、鍵暗号化手段６３へ送る。鍵暗号化手段６３は、ＶＴＲ情報記憶手段７１に記憶されている共通鍵Ｋｃを用いて、ワークキーＫｗに暗号化を施して、暗号化ワークキーＫｃ（Ｋｗ）を生成する。

【００９８】

分離された暗号化ＡＶデータＫｗ（Ｄ）は、Ｄ－Ｉ／Ｆ５１を介して、生成された暗号化ワークキーＫｃ（Ｋｗ）は、認証鍵交換部５２およびＤ－Ｉ／Ｆ５１を介して、それぞれＳＴＢ１へ伝達されるが、それに先だって、記録時と同様に、ＳＴＢ１、ＶＴＲ装置５それぞれの認証鍵交換部１９、５２は、Ｄ－Ｉ／Ｆ１８および５１を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

【００９９】

ＳＴＢ１へ伝達された暗号化ＡＶデータＫｗ（Ｄ）は、Ｄ－Ｉ／Ｆ１８を介して、暗号解読手段１４へ送られ、暗号化ワークキーＫｃ（Ｋｗ）は、Ｄ－Ｉ／Ｆ１８および認証鍵交換部１９を介して、鍵復元手段３２へ送られる。鍵復元手段３２は、ＳＴＢ情報記憶手段１１に記憶されている共通鍵Ｋｃを用いて、暗号化ワークキーＫｃ（Ｋｗ）をワークキーＫｗに復元して、暗号解読手段１４へ送る。暗号解読手段１４は、復元されたワークキーＫｗを用いて、暗号化ＡＶデータＫｗ（Ｄ）を解読して得られるＡＶデータＤを、デコーダ１２へ出力する。デコーダ１２は、ＡＶデータＤに施された高能率符号化処理等をデコードし、モニター４へ出力する。

【０１００】

以上の手順にしたがって、ＡＶデータを記録／再生することにより、ＡＶデータに暗号化を施すのに用いたワークキーにＶＴＲ装置５に固有の公開鍵を用いて暗号化を施して、暗号化されたＡＶデータと一緒に記録媒体に記録し、再生時には暗号化されたワークキーをＶＴＲ装置５に固有の秘密鍵を用いて復元しているため、ＶＴＲ装置５に固有の秘密鍵を持っているシステム、すなわち、ＶＴＲ装置５そのものを備えているシステムしか再生できないので、本実施の形態におけるデータ記録再生システムは、特定の対象に対してのみ、再生が可能であり、暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムであることがわかる。

【０１０１】

なお、本実施の形態におけるデータ記録再生システムから、図１８に示すように、鍵暗号化手段３１、鍵復元手段３２、鍵復元手段６１および鍵暗号化手段６３を省略した構成も可能である。こうすれば、本発明のチューナ装置とＶＴＲ装置との間のデータ送信において、ワークキーに暗号化を施さずに送信を行うことになる。以下に、図１３の構成のデータ記録再生システムについて説明する。

【０１０２】

図１８の構成のデータ記録再生システムにおける、ＡＶデータを記録媒体６に記録する時のデータの流れは、図１９に示すようになる。図１９において、図１８で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。また、図中の記号については、図１６、図１７に倣う。

【０１０３】

放送用電波として暗号化され、多重化されたＡＶデータＤは、アンテナ３を介して受信され、受信復調部２１で復調され、放送用の暗号を放送用暗号解除部２２で解除され、ＤＭＵＸ２３で分離されて、生のＡＶデータＤとなって、デコーダ１２および暗号化手段１３へ送られる。デコーダ１２は、ＡＶデータＤに施された高能率符号化処理等をデコードし、モニター４へ出力する。暗号化手段１３は、ワークキーＫｗを生成し、生成したワークキーＫｗを用いて、ＡＶデータＤに暗号化を施して、暗号化ＡＶデータＫｗ（Ｄ）を生成する。

【０１０４】

暗号化ＡＶデータＫｗ（Ｄ）は、Ｄ－Ｉ／Ｆ１８を介して、ワークキーＫｗは、認証鍵交換部１９およびＤ－Ｉ／Ｆ１８を介して、それぞれＶＴＲ装置５へ伝達されるが、それに先だって、ＳＴＢ１、ＶＴＲ装置５それぞれの認証鍵交換部１９、５２は、Ｄ－Ｉ／Ｆ１８および５１を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

【０１０５】

ＶＴＲ装置５へ伝達された暗号化ＡＶデータＫｗ（Ｄ）は、Ｄ－Ｉ／Ｆ５１を介して、ＭＵＸ５４へ送られる。また、ＶＴＲ装置５へ伝達されたワークキーＫｗは、Ｄ－Ｉ／Ｆ５１および認証鍵交換部５２を介して、鍵暗号化手段６２に送られる。鍵暗号化手段６２は、ＶＴＲ情報記憶手段７１に記憶されているＶＴＲ装置５に固有の公開鍵 $_{VTR}$Ｐａを用いて、ワークキーＫｗに暗号化を施して、暗号化ワークキー $_{VTR}$Ｐａ（Ｋｗ）を生成して、これをＭＵＸ５４へ送る。ＭＵＸ５４へ送られた暗号化ＡＶデータＫｗ（Ｄ）および暗号化ワークキー $_{VTR}$Ｐａ（Ｋｗ）は、記録媒体６のフォーマットに適合した多重化を行われた後、記録処理部５５によって、記録媒体６に記録される。

【０１０６】

次に、図１８の構成のデータ記録再生システムにおける、記録媒体６に記録されたＡＶデータを再生する時のデータの流れを図２０を用いて説明する。図２０において、図１８で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。また、図中の記号については、図１６、図１７に倣う。

【０１０７】

多重化されて記録媒体６に記録された暗号化ＡＶデータＫｗ（Ｄ）および暗号化ワークキー $_{VTR}$Ｐａ（Ｋｗ）は、再生処理部５８により再生され、ＤＭＵＸ５７で分離される。分離された暗号化ワークキー $_{VTR}$Ｐａ（Ｋｗ）は、鍵復元手段６４へ送られる。鍵復元手段６４は、ＶＴＲ情報記憶手段７１に記憶されているＶＴＲ装置５に固有の秘密鍵 $_{VTR}$Ｓａを用いて、暗号化ワークキー $_{VTR}$Ｐａ（Ｋｗ）をワークキーＫｗに復元する。

【０１０８】

分離された暗号化ＡＶデータＫｗ（Ｄ）は、Ｄ－Ｉ／Ｆ５１を介して、復元さ

れたワークキーＫｗは、認証鍵交換部５２およびＤ－Ｉ／Ｆ５１を介して、それぞれＳＴＢ１へ伝達されるが、それに先だって、記録時と同様に、ＳＴＢ１、ＶＴＲ装置５それぞれの認証鍵交換部１９、５２は、Ｄ－Ｉ／Ｆ１８および５１を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

【０１０９】

ＳＴＢ１へ伝達された暗号化ＡＶデータＫｗ（Ｄ）は、Ｄ－Ｉ／Ｆ１８を介して、暗号解読手段１４へ送られ、ワークキーＫｗは、Ｄ－Ｉ／Ｆ１８および認証鍵交換部１９を介して、それぞれ暗号解読手段１４へ送られる。暗号解読手段１４は、ワークキーＫｗを用いて、暗号化ＡＶデータＫｗ（Ｄ）を解読して得られるＡＶデータＤを、デコーダ１２へ出力する。デコーダ１２は、ＡＶデータＤに施された高能率符号化処理等をデコードし、モニター４へ出力する。

【０１１０】

なお、ＳＴＢ情報記憶手段１１およびＶＴＲ情報記憶手段７１は、図１５の構成において保持していた共通鍵の情報を保持している必要はない。

【０１１１】

以上の手順にしたがって、ＡＶデータを記録／再生することにより、ＳＴＢ１とＶＴＲ装置５との間のデータ送信において、ワークキーに暗号化を施さずに送信を行うので、記録／再生時のＳＴＢ１およびＶＴＲ装置５の負担をさらに軽減できるので、図１８の構成のデータ記録再生システムは、図１５の構成のデータ記録再生システムと比較して、さらに記録効率の向上を図ることが可能なシステムであることがわかる。ただし、図１５の構成のデータ記録再生システムと比較して、ＳＴＢ１とＶＴＲ装置５との間のデータ送信についてのセキュリティは低下する。このような構成は、後述する第８の実施の形態のように、ＳＴＢおよびＶＴＲ装置の機能を一体化した一体化ＳＴＢを備えるデータ記録再生システムに適用すると、特に有効である。

【０１１２】

（第７の実施の形態）

以下に、本発明の第７の実施の形態を図面を参照して説明する。本実施の形態

が上述した第１の実施の形態と異なる点は、公開鍵および秘密鍵を用いる替わりに、共通鍵を用いてワークキーの暗号化／復元を行う点である。したがって、本実施の形態において、第１の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第１の実施の形態と同じとする。

【０１１３】

本実施の形態におけるデータ記録再生システムの構成は、第１の実施の形態におけるデータ記録再生システムの構成と同じである。

【０１１４】

次に、このような本実施の形態の動作を説明する。

【０１１５】

図２１は、本発明の第７の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図であり、図２２は、本発明の第７の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図２１、図２２に示すとおり、本実施の形態においては、ワークキーＫｗの暗号化および復元にＳＴＢ情報記憶手段１１に保持されている共通鍵Ｋｃを用いている点以外は、第１の実施の形態におけるデータ記録再生システムと同じである。なお、共通鍵Ｋｃは、例えば、ＳＴＢ１もしくはＳＴＢ１の機器モデル、ユーザＩＤ、サービスいずれかに対して固有な鍵である。また、共通鍵Ｋｃは、ＩＣカード２に記録されているとしてもよい。共通鍵ＫｃがＩＣカード２に記録されていない場合で、課金情報が、例えば、ＳＴＢ情報記憶手段１１に記録される場合は、カード読取手段１０を省略してもよい。また、共通鍵ＫｃがＳＴＢ記憶手段１１に記録されていない場合は、ＳＴＢ記憶手段１１を省略してもよい。

【０１１６】

以上の手順にしたがって、ＡＶデータを記録／再生することにより、ワークキーに暗号化に公開鍵を用いないので、本実施の形態におけるデータ記録再生システムは、第１の実施の形態におけるデータ記録再生システムと比較して、鍵自身のデータ長を短くでき、記録効率の向上および装置の小型化を図ることが可能な

システムであることがわかる。

【０１１７】

（第８の実施の形態）

以下に、本発明の第８の実施の形態を図面を参照して説明する。本実施の形態が上述した第１の実施の形態と異なる点は、第１の実施の形態におけるデータ記録再生システムが本発明のチューナ装置およびＶＴＲ装置を備えていたのに対し、本実施の形態におけるデータ記録再生システムが前記チューナ装置および前記ＶＴＲ装置の機能が一体化された装置を備えていることに関する点である。したがって、本実施の形態において、第１の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第１の実施の形態と同じとする。

【０１１８】

図２３は、本発明の第８の実施の形態におけるデータ記録再生システムの構成を示す構成図である。本実施の形態におけるデータ記録再生システムの構成が、第１の実施の形態におけるデータ記録再生システムの構成と異なるのは、ＳＴＢ１およびＶＴＲ装置５の機能を一体化した一体化ＳＴＢ７を備えることによって、第１の実施の形態におけるデータ記録再生システムが備えていたＶＴＲ伝達手段１７およびＳＴＢ伝達手段５０を省略したことである。

【０１１９】

なお、第１の実施の形態と同様に、課金情報が、例えば、ＳＴＢ情報記憶手段１１に記録される場合は、本実施の形態の構成におけるデータ記録再生システムから、ＩＣカード２およびカード読取手段１０を省いてもよい。

【０１２０】

次に、このような本実施の形態の動作を説明する。

【０１２１】

まず、ＡＶデータを記録媒体６に記録する時のデータの流れを図２４を用いて説明する。図２４は、本発明の第８の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。図２４において、図２３で示した構成のうち、記録時に不要な手段等は、適宜省略して示す。また、図

中の記号については、図２、図３に倣うが、 $_{STB}$Ｐａは、ワークキーＫｗの暗号化に用いる一体化ＳＴＢ７に固有の公開鍵を示す。なお、本実施の形態におけるデータ記録再生システムは、第１の実施の形態と同様に、ワークキーＫｗを、定期的または不定期的に切り替えることによって、切り替えない場合に比して、さらに、暗号化に関する情報が外部に漏洩しにくいシステムとなっている。

【０１２２】

放送用電波として暗号化され、多重化されたＡＶデータＤは、アンテナ３を介して受信され、受信復調部２１で復調され、放送用の暗号を放送用暗号解除部２２で解除され、ＤＭＵＸ２３で分離されて、生のＡＶデータＤとなって、デコーダ１２および暗号化手段１３へ送られる。デコーダ１２は、ＡＶデータＤに施された高能率符号化処理等をデコードし、モニター４へ出力する。暗号化手段１３は、ワークキーＫｗを生成し、生成したワークキーＫｗを用いて、ＡＶデータＤに暗号化を施して、暗号化ＡＶデータＫｗ（Ｄ）を生成する。生成されたワークキーＫｗは、鍵暗号化手段１５へ送られ、鍵暗号化手段１５は、ＳＴＢ情報記憶手段１１に記憶されている一体化ＳＴＢ７に固有の公開鍵 $_{STB}$Ｐａを用いて、ワークキーＫｗに暗号化を施して、暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ）を生成する。

【０１２３】

生成された暗号化ＡＶデータＫｗ（Ｄ）および暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ）は、それぞれＭＵＸ５４へ送られて、記録媒体６のフォーマットに適合した多重化を行われた後、記録処理部５５によって、記録媒体６に記録される。

【０１２４】

次に、記録媒体６に記録されたＡＶデータを再生する時のデータの流れを図２５を用いて説明する。図２５は、本発明の第８の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図２５において、図２３で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。図中の記号は、図２、図３に倣うが、 $_{STB}$Ｓａは、公開鍵 $_{STB}$Ｐａに対応し、暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ）を解読してワークキーＫｗを復元するのに用いる一体化ＳＴＢ７に固有の秘密鍵を示す。

【０１２５】

多重化されて記録媒体６に記録された暗号化ＡＶデータＫｗ（Ｄ）および暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ）は、再生処理部５８により再生され、ＤＭＵＸ５７で分離される。

【０１２６】

分離された暗号化ＡＶデータＫｗ（Ｄ）は、暗号解読手段１４へ送られ、分離された暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ）は、鍵復元手段１６へ送られる。鍵復元手段１６は、ＳＴＢ情報記憶手段１１に記憶されている一体化ＳＴＢ７に固有の秘密鍵 $_{STB}$Ｓａを用いて、暗号化ワークキー $_{STB}$Ｐａ（Ｋｗ）をワークキーＫｗに復元して、暗号解読手段１４へ送る。暗号解読手段１４は、復元されたワークキーＫｗを用いて、暗号化ＡＶデータＫｗ（Ｄ）を解読して得られるＡＶデータＤを、デコーダ１２へ出力する。デコーダ１２は、ＡＶデータＤに施された高能率符号化処理等をデコードし、モニター４へ出力する。

【０１２７】

以上の手順にしたがって、ＡＶデータを記録／再生することにより、各装置間のデータ伝達にかかる負担を省略できるので、本実施の形態におけるデータ記録再生システムは、特定の対象に対してのみ、再生が可能であり、暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムであり、かつ、第１の実施の形態におけるデータ記録再生システムと比較して、さらに記録効率の向上を図ることが可能なシステムであることがわかる。

なお、本発明の公開鍵および秘密鍵は、本実施の形態においては、一体化ＳＴＢ７に対して固有な鍵であるとして説明したが、これに限るものではなく、例えば、第２～第４いずれかの実施の形態と同様に、一体化ＳＴＢ７の機器モデルに対して固有な鍵、本発明のＩＣカードに記録されたユーザＩＤに対して固有な鍵、本発明のＩＣカードに記録されたサービスに対して固有な鍵であってもよい。

【０１２８】

なお、本発明のワークキーは、上述した第１～第８の実施の形態においては、定期的または不定期的に切り替えられるとして説明したが、同じワークキーを用いるとすると、定期的または不定期的に切り替える場合と比較して、暗号化に関

する情報が外部に漏洩するおそれが高くなるが、従来のデータ記録再生システムと比較すると、暗号化に関する情報が外部に漏洩しにくいシステムであるといえる。

【０１２９】

また、本発明の第２の暗号化は、上述した第１～第８の実施の形態においては、本発明の第１の暗号化において用いたワークキーとは別の鍵（公開鍵、共通鍵）であるとして説明したが、これに限るものではなく、第１の暗号化に用いたワークキーに対応するアルゴリズムと同じアルゴリズムを用いて、当該ワークキー自身に第２の暗号化を施すとしてもよい。また、例えば、ワークキーとして共通鍵を用いてディジタルデータに第１の暗号化を施し、当該共通鍵に同じ共通鍵を用いて第２の暗号化を施すとしてもよい。

【０１３０】

なお、上述した第１～第８の実施の形態においては、本発明のデータ記録再生システムを中心に説明したが、本発明のデータ記録再生方法は、上記説明中で、説明された方法である。

【０１３１】

【発明の効果】

以上説明したところから明らかなように、請求項１の本発明は、データに暗号化を施すことによって、特定の対象に対してのみ、再生が可能であり、前記暗号化に関する情報が外部に漏洩しにくいデータ記録再生方法を提供することができる。また、請求項４の本発明は、データに暗号化を施すことによって、特定の対象に対してのみ、再生が可能であり、前記暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムを提供することができる。また、請求項２２または２３の本発明は、記録および／または再生時に、確実に課金が可能なデータ記録再生方法およびデータ記録再生システムを提供することができる。さらに、請求項３０の本発明は、再生時のロスタイムが少ないデータ記録再生システムを提供することができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施の形態におけるデータ記録再生システムの構成を示す構成図である。

【図２】

本発明の第１の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

【図３】

本発明の第１の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

【図４】

本発明の第１の実施の形態におけるデータ記録再生システムを用いて記録された記録媒体上の記録領域を示す模式図である。

【図５】

本発明の第２の実施の形態におけるデータ記録再生システムで記録された記録媒体の貸与時の流れを示すフロー図である。

【図６】

本発明の第３の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

【図７】

本発明の第３の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

【図８】

本発明の第４の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

【図９】

本発明の第４の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

【図１０】

本発明の第５の実施の形態におけるデータ記録再生システムの構成を示す構成図である。

【図１１】

本発明の第５の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

【図１２】

本発明の第５の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

【図１３】

本発明の第５の実施の形態における別のデータ記録再生システムの構成を示す構成図である。

【図１４】

本発明の第５の実施の形態における別のデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

【図１５】

本発明の第６の実施の形態におけるデータ記録再生システムの構成を示す構成図である。

【図１６】

本発明の第６の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

【図１７】

本発明の第６の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

【図１８】

本発明の第６の実施の形態における別のデータ記録再生システムの構成を示す構成図である。

【図１９】

本発明の第６の実施の形態における別のデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

【図２０】

本発明の第６の実施の形態における別のデータ記録再生システムのデータ再生

時のデータの流れを示すフロー図である。

【図２１】

本発明の第７の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

【図２２】

本発明の第７の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

【図２３】

本発明の第８の実施の形態におけるデータ記録再生システムの構成を示す構成図である。

【図２４】

本発明の第８の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

【図２５】

本発明の第８の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

【図２６】

従来の衛星放送のデータ記録再生システムを示す構成図である。

【符号の説明】

１、１０１、９０１　ＳＴＢ

２、１０２、９０２　ＩＣカード

３、９０３　アンテナ

４、９０４　モニター

５、１０５、９０５　ＶＴＲ装置

６、９０６　記録媒体

７　一体化ＳＴＢ

１０　カード読取手段

１１　ＳＴＢ情報記憶手段

１２　デコーダ

１３　暗号化手段

１４　暗号解読手段

１５、３１、６２、６３　鍵暗号化手段

１６、３２、６１、６４　鍵復元手段

１７　ＶＴＲ伝達手段

１８、５１　Ｄ－Ｉ／Ｆ

１９、５２　認証鍵交換部

２０　受信手段

２１　受信復調部

２２　放送用暗号解除部

２３、５７　ＤＭＵＸ

５０　ＳＴＢ伝達手段

５３　記録手段

５４　ＭＵＸ

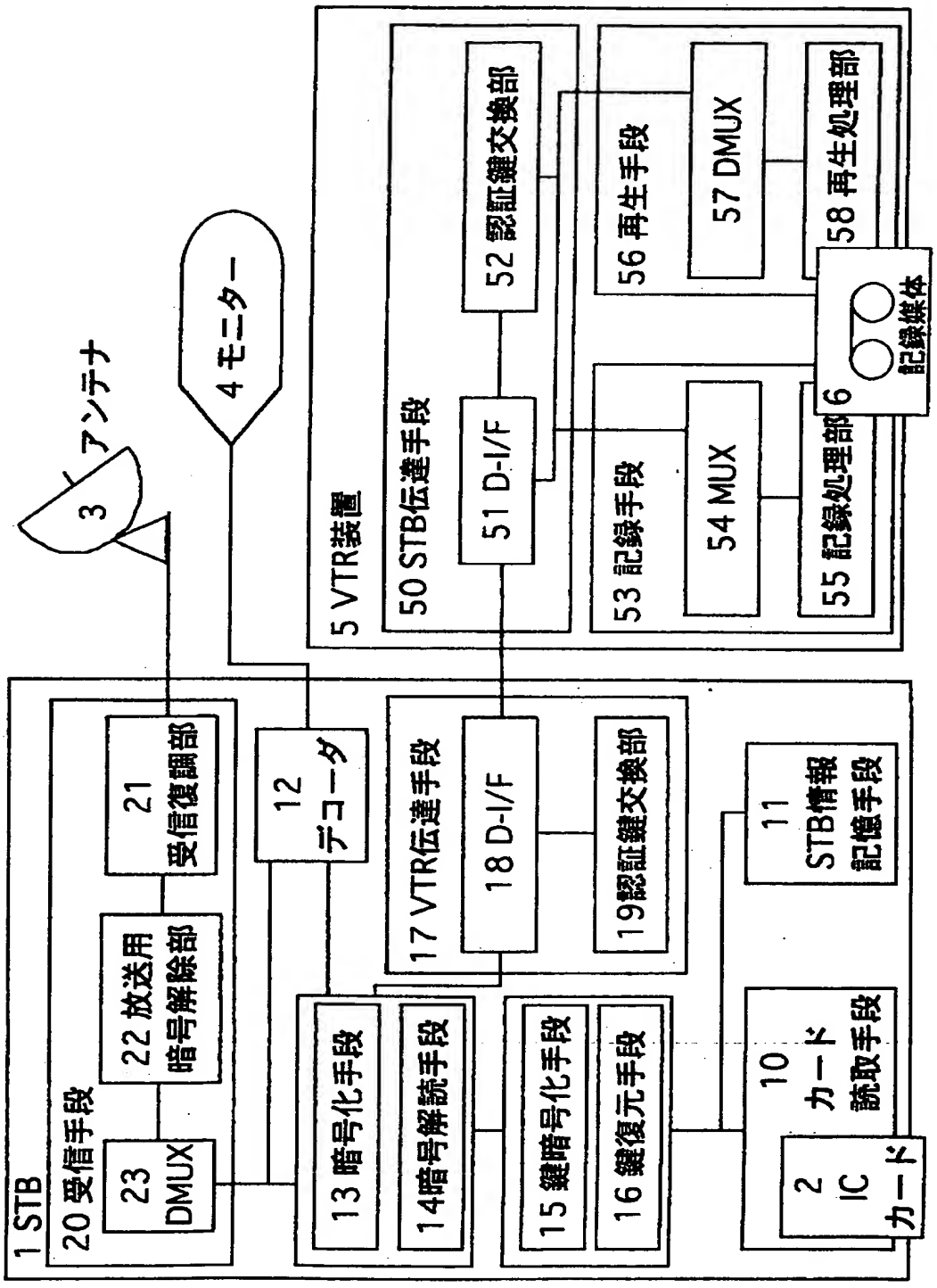
５５　記録処理部

５６　再生手段

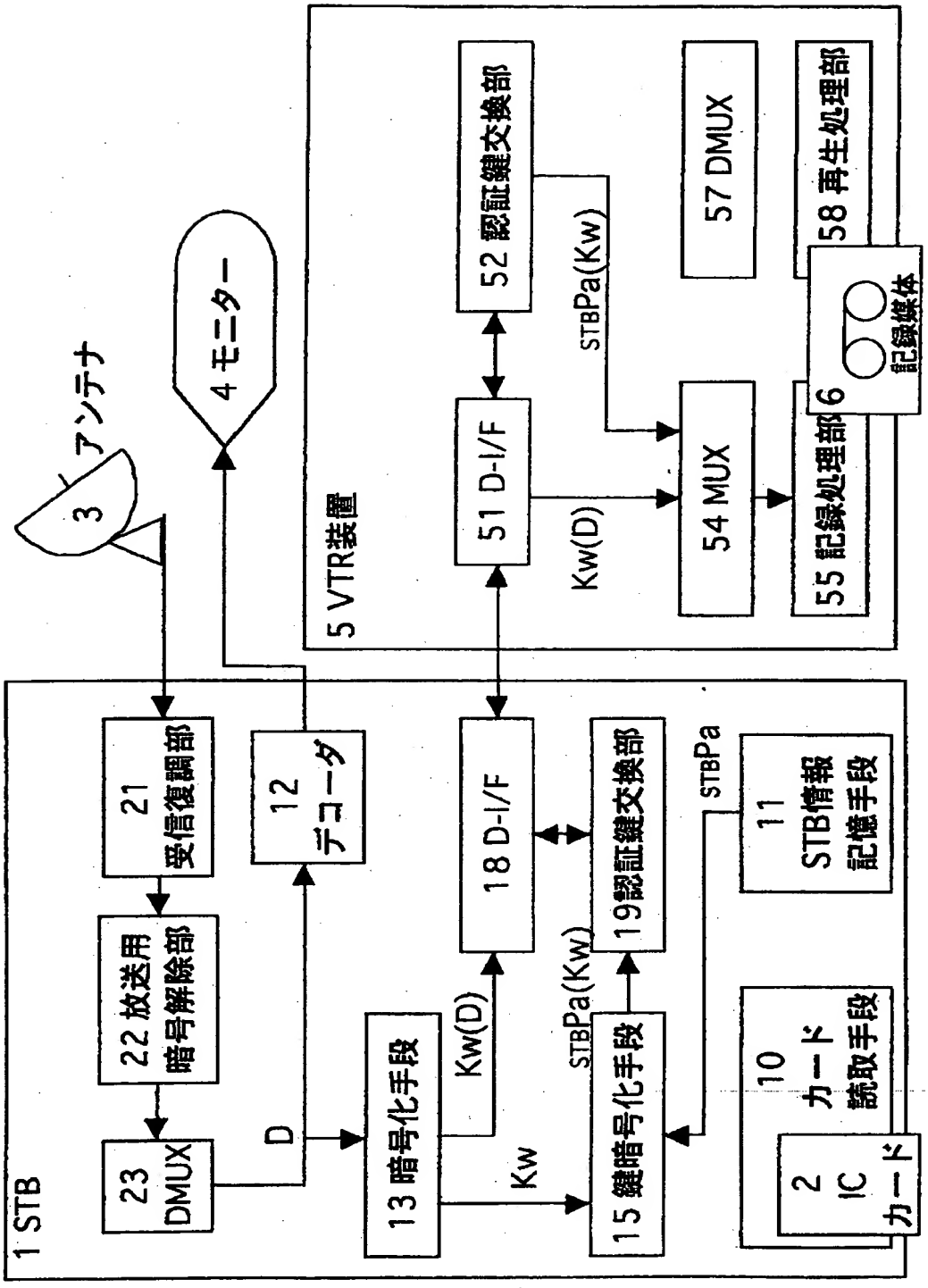
５８　再生処理部

【書類名】　図面

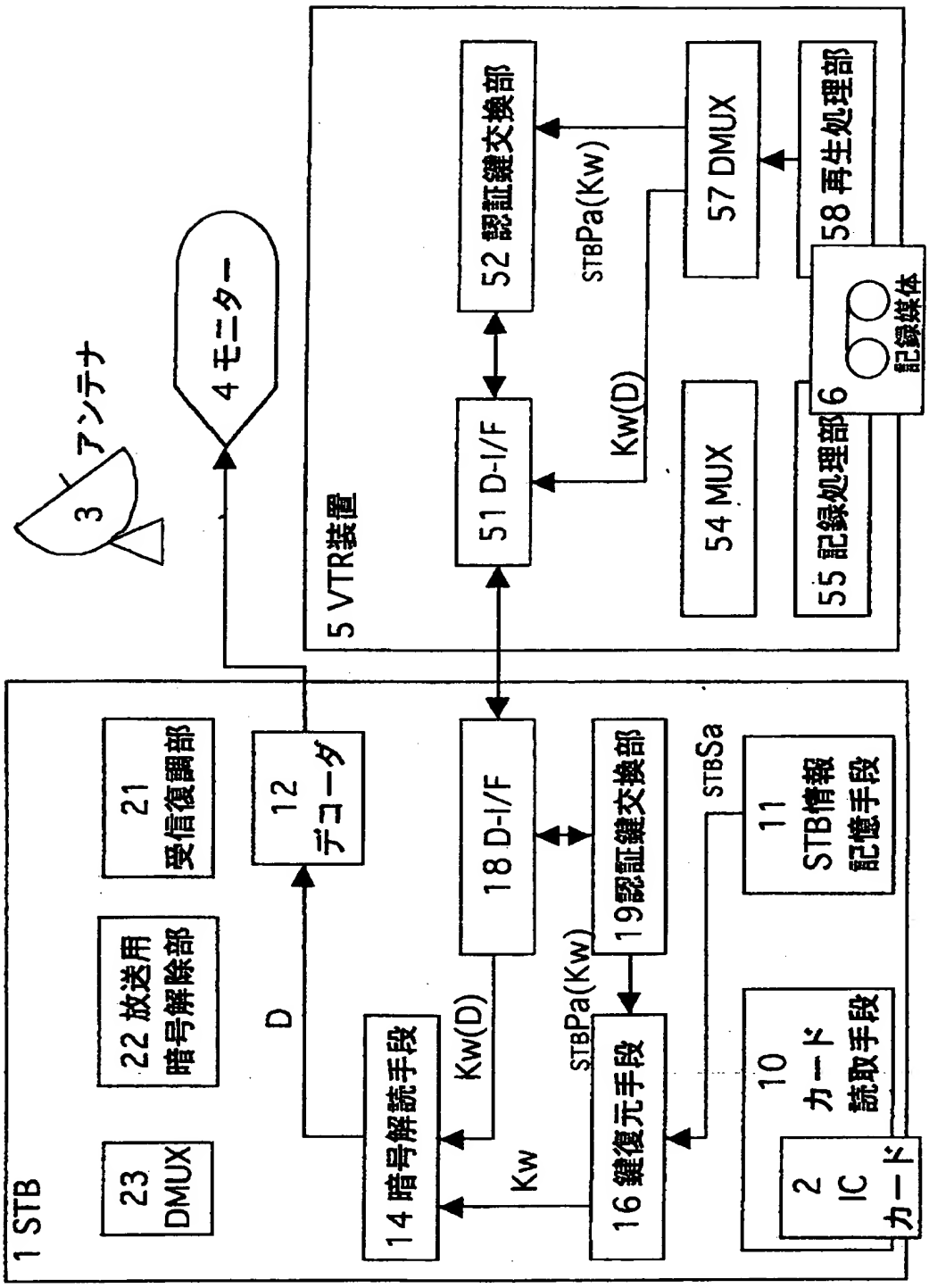
【図１】


1 STB
20 受信手段
21 受信復調部
22 放送用 暗号解除部
23 DMUX
12 デコーダ
13 暗号化手段
14暗号解読手段
15 鍵暗号化手段
16 鍵復元手段
17 VTR伝達手段
18 D-I/F
19認証鍵交換部
10 カード 読取手段
2 IC カード
11 STB情報 記憶手段
3 アンテナ
4 モニター
5 VTR装置
50 STB伝達手段
51 D-I/F
52 認証鍵交換部
53 記録手段
54 MUX
55 記録処理部
56 再生手段
57 DMUX
58 再生処理部
6 記録媒体

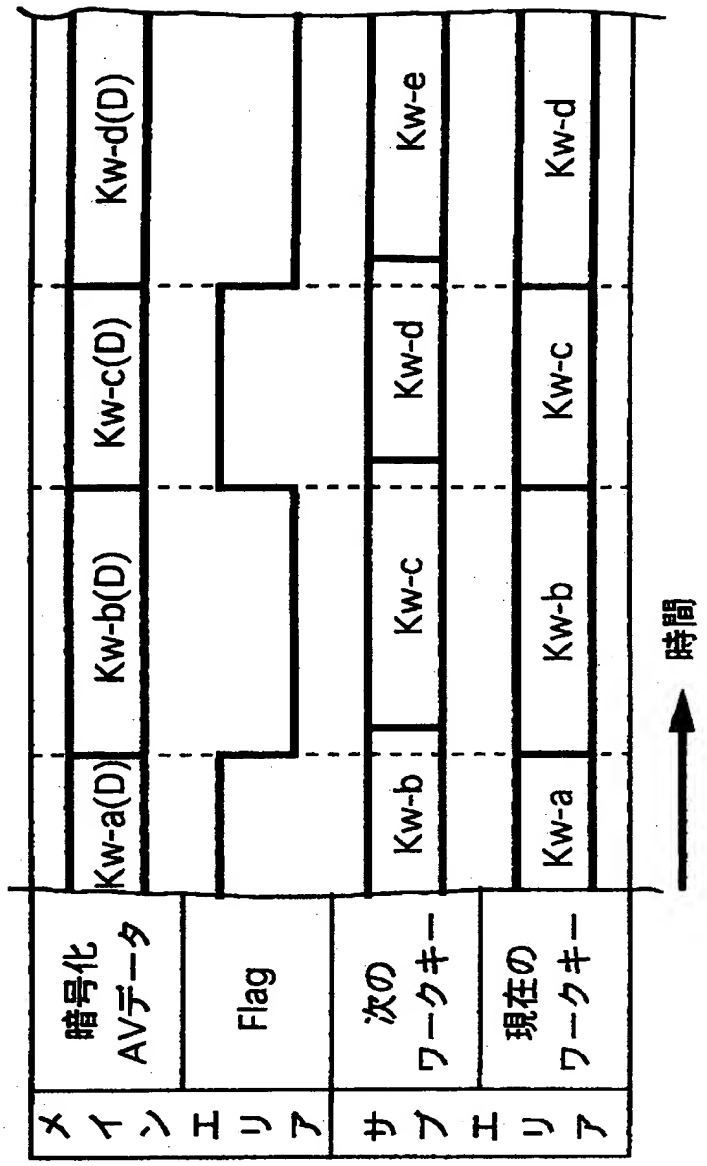
【図２】


1 STB
2 IC カード
3 アンテナ
4 モニター
5 VTR装置
6 記録媒体
10 カード読取手段
11 STB情報記憶手段
12 デコーダ
13 暗号化手段
15 鍵暗号化手段
18 D-I/F
19認証鍵交換部
21 受信復調部
22 放送用暗号解除部
23 DMUX
51 D-I/F
52 認証鍵交換部
54 MUX
55 記録処理部
57 DMUX
58 再生処理部
D
Kw
Kw(D)
STBPa
STBPa(Kw)

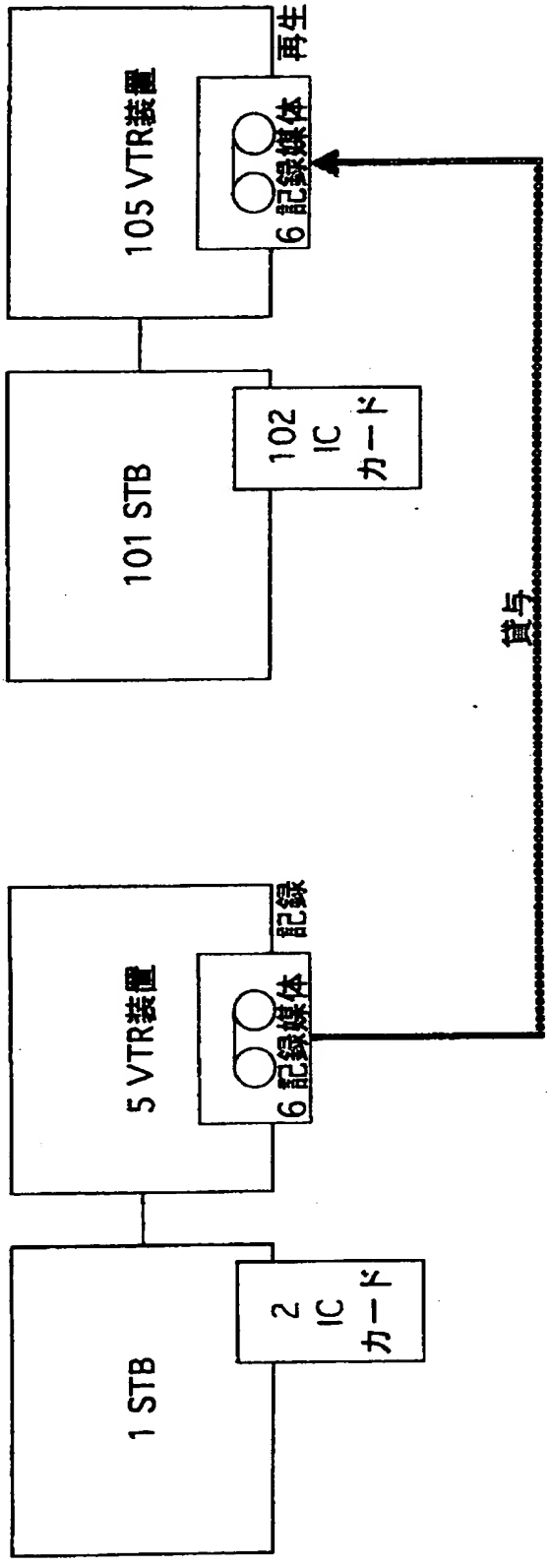
【図３】


1 STB
23 DMUX
22 放送用 暗号解除部
21 受信復調部
12 デコーダ
D
14 暗号解読手段
Kw
Kw(D)
18 D-I/F
STBPa(Kw)
19認証鍵交換部
16 鍵復元手段
STBSa
11 STB情報 記憶手段
10 カード 読取手段
2 IC カード
3 アンテナ
4 モニター
5 VTR装置
51 D-I/F
Kw(D)
52 認証鍵交換部
STBPa(Kw)
54 MUX
57 DMUX
55 記録処理部
58 再生処理部
6 記録媒体

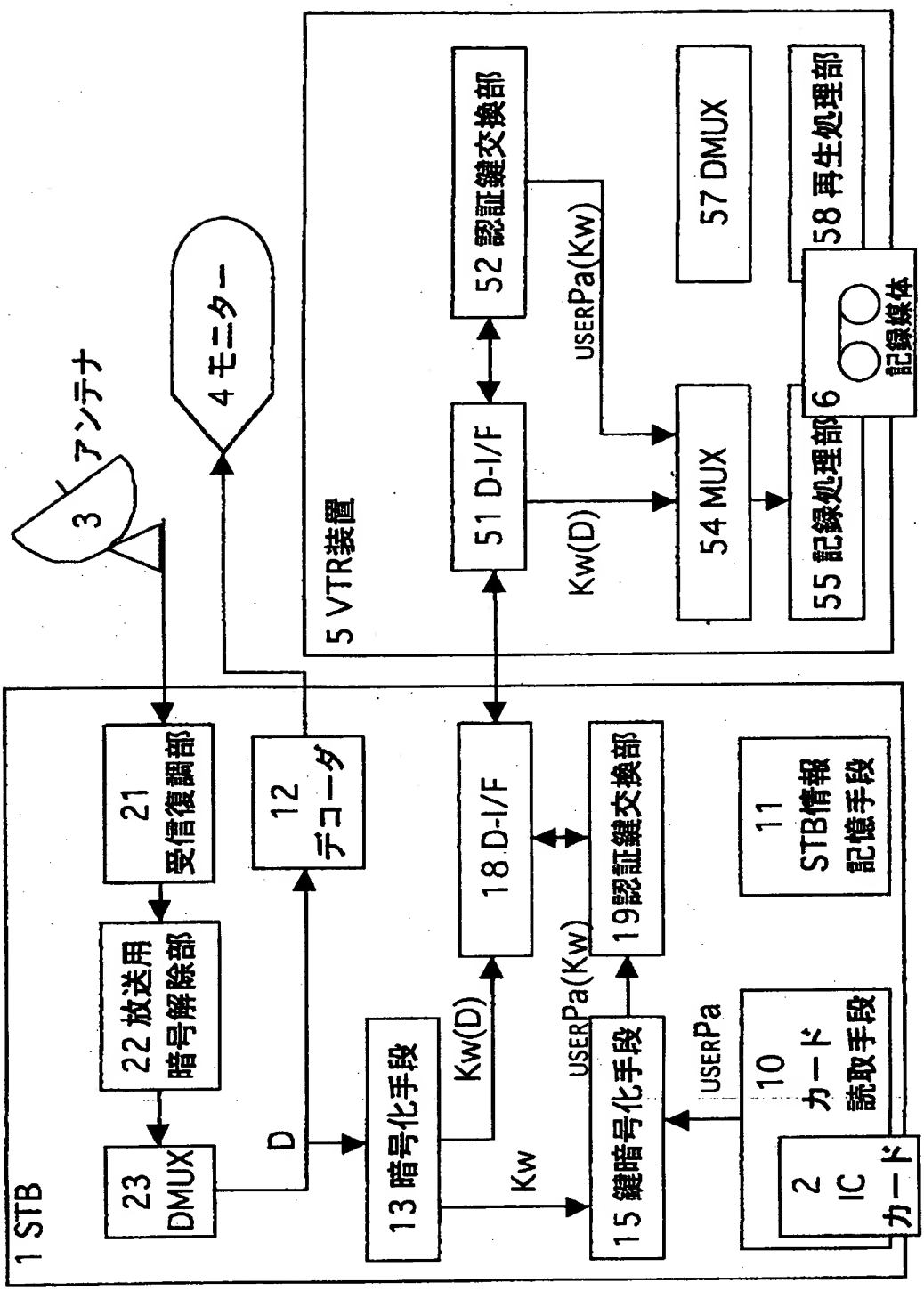
【図４】


メインエリア
サブエリア
暗号化AVデータ
Flag
次のワークキー
現在のワークキー
Kw-a(D)
Kw-b(D)
Kw-c(D)
Kw-d(D)
Kw-b
Kw-c
Kw-d
Kw-e
Kw-a
Kw-b
Kw-c
Kw-d
時間

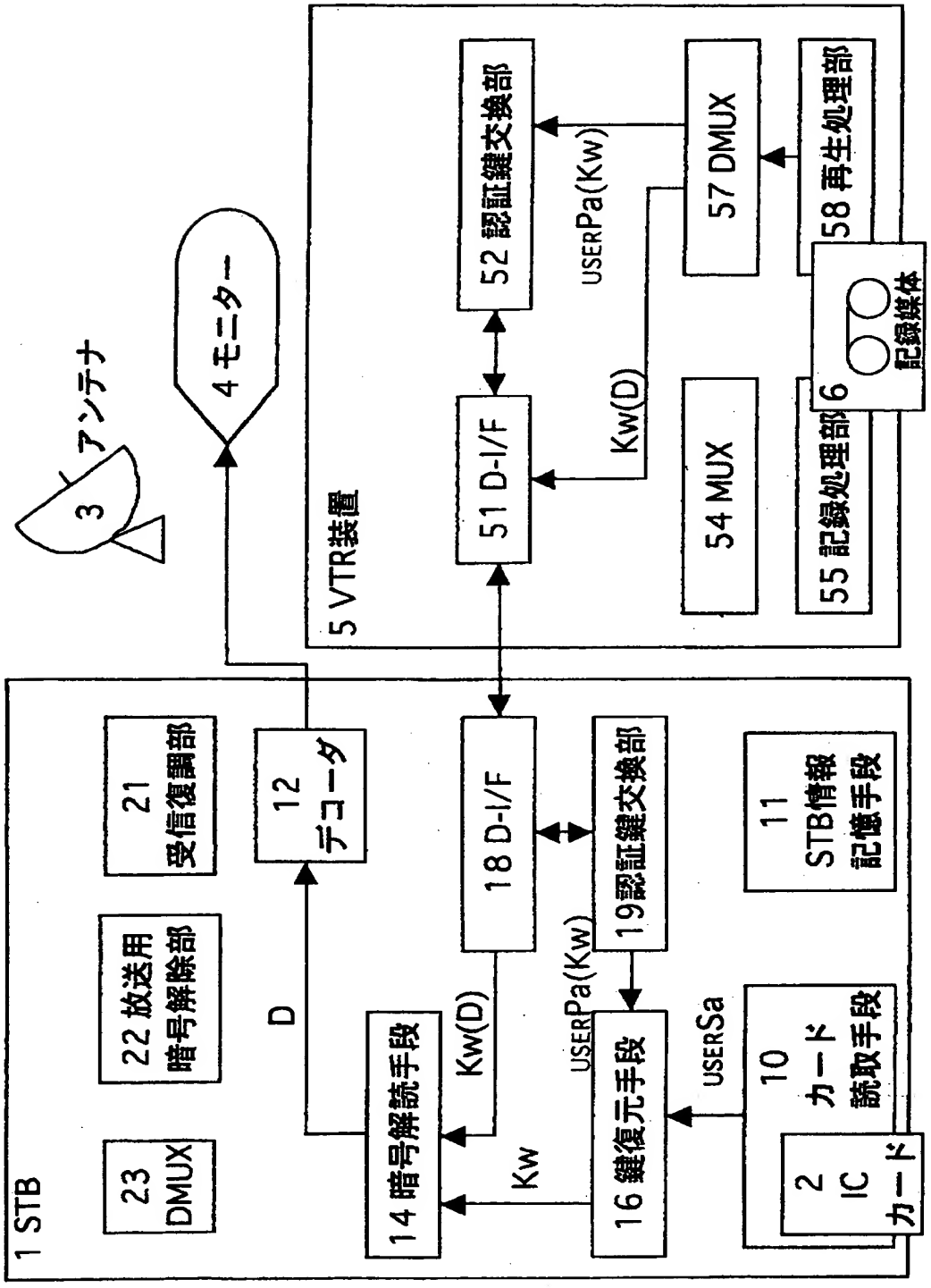
【図５】


105 VTR装置
再生
6 記録媒体
101 STB
102 ICカード
貸与
5 VTR装置
記録
6 記録媒体
1 STB
2 ICカード

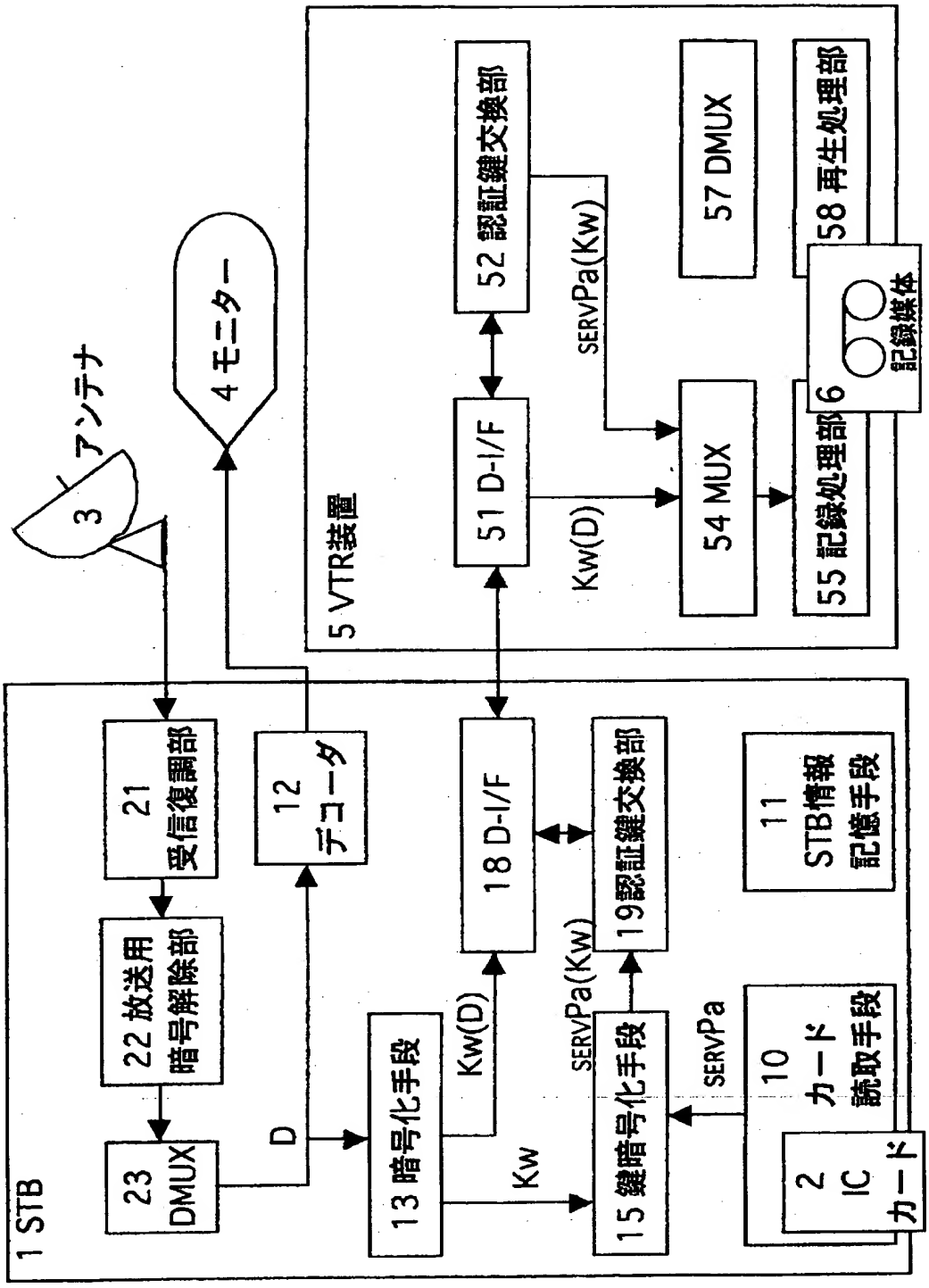
【図６】


1 STB
2 IC カード
10 カード読取手段
11 STB情報記憶手段
12 デコーダ
13 暗号化手段
15 鍵暗号化手段
18 D-I/F
19認証鍵交換部
21 受信復調部
22 放送用暗号解除部
23 DMUX
3 アンテナ
4 モニター
5 VTR装置
51 D-I/F
52 認証鍵交換部
54 MUX
55 記録処理部
57 DMUX
58 再生処理部
6 記録媒体
D
Kw
Kw(D)
USERPa
USERPa(Kw)
Kw(D)

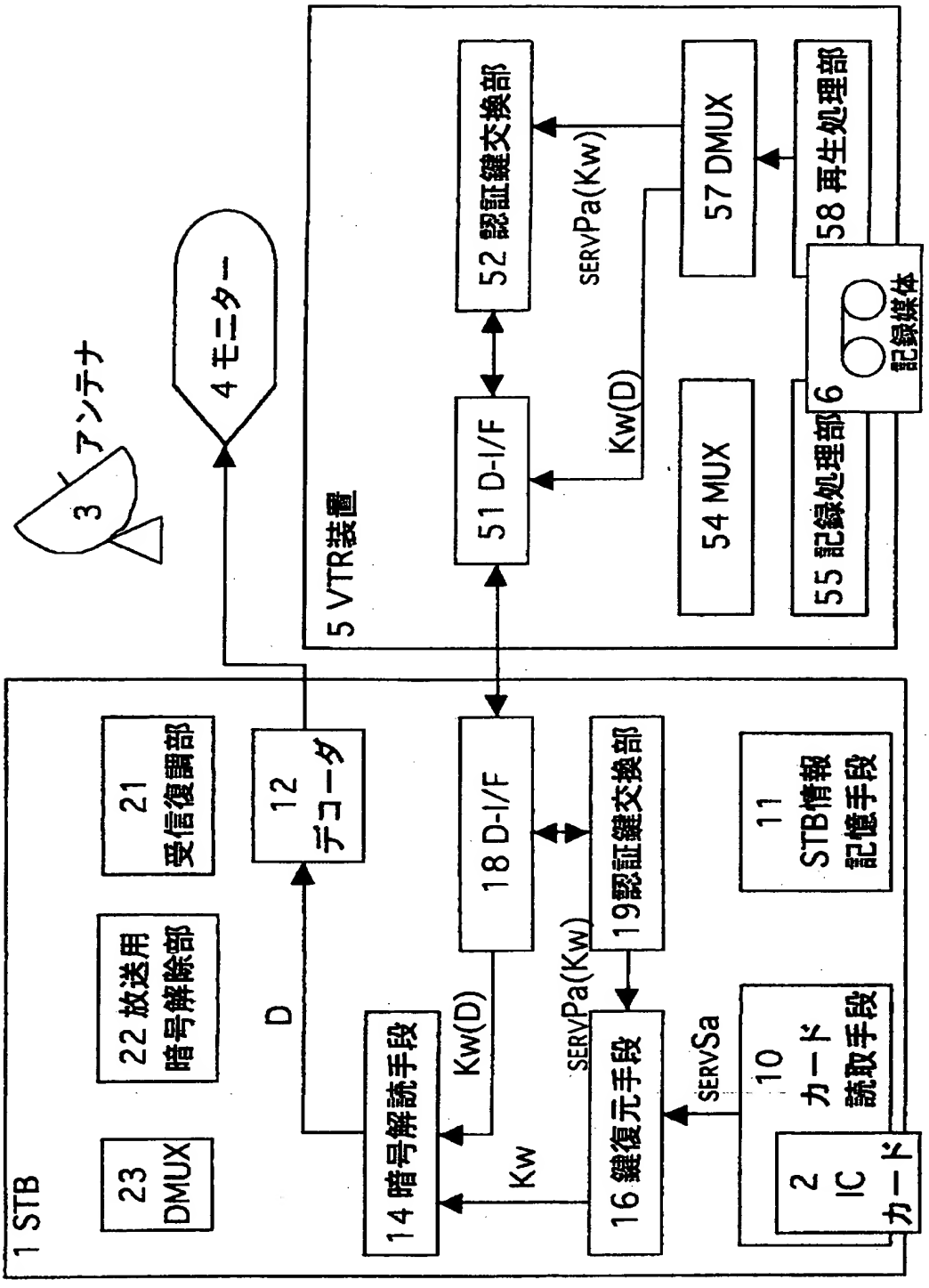
【図７】


1 STB
2 IC カード
10 カード読取手段
11 STB情報記憶手段
12 デコーダ
14 暗号解読手段
16 鍵復元手段
18 D-I/F
19認証鍵交換部
21 受信復調部
22 放送用暗号解除部
23 DMUX
3 アンテナ
4 モニター
5 VTR装置
51 D-I/F
52 認証鍵交換部
54 MUX
55 記録処理部
57 DMUX
58 再生処理部
6 記録媒体
D
Kw
Kw(D)
USERPa(Kw)
USERSa

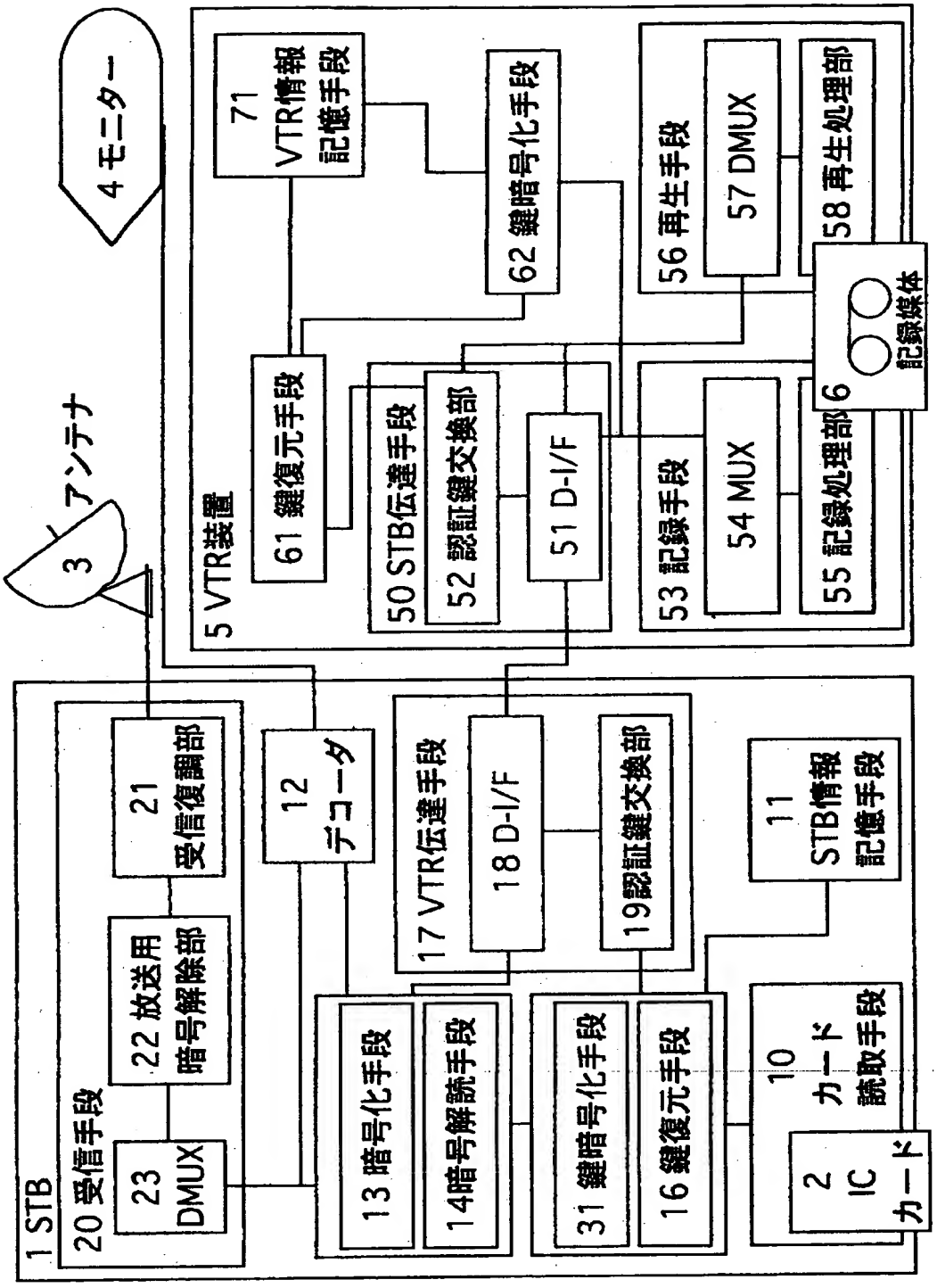
【図８】


1 STB
2 IC カード
3 アンテナ
4 モニター
5 VTR装置
6 記録媒体
10 カード 読取手段
11 STB情報 記憶手段
12 デコーダ
13 暗号化手段
15 鍵暗号化手段
18 D-I/F
19認証鍵交換部
21 受信復調部
22 放送用 暗号解除部
23 DMUX
51 D-I/F
52 認証鍵交換部
54 MUX
55 記録処理部
57 DMUX
58 再生処理部
D
Kw
Kw(D)
SERVPa
SERVPa(Kw)

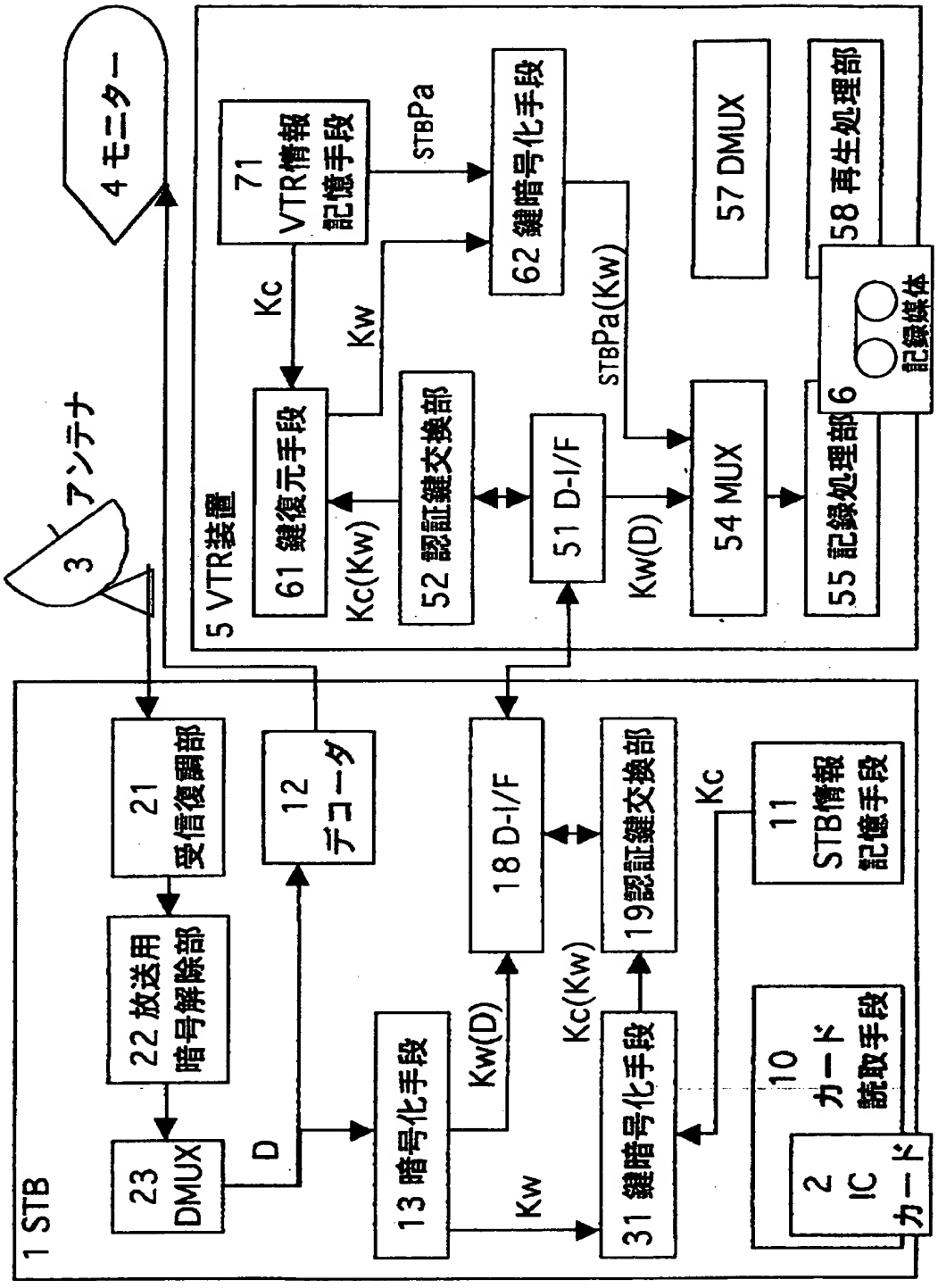
【図９】


1 STB
2 IC カード
10 カード読取手段
11 STB情報記憶手段
12 デコーダ
14 暗号解読手段
16 鍵復元手段
18 D-I/F
19認証鍵交換部
21 受信復調部
22 放送用暗号解除部
23 DMUX
3 アンテナ
4 モニター
5 VTR装置
51 D-I/F
52 認証鍵交換部
54 MUX
55 記録処理部
57 DMUX
58 再生処理部
6 記録媒体
D
Kw
Kw(D)
SERVPa(Kw)
SERVSa

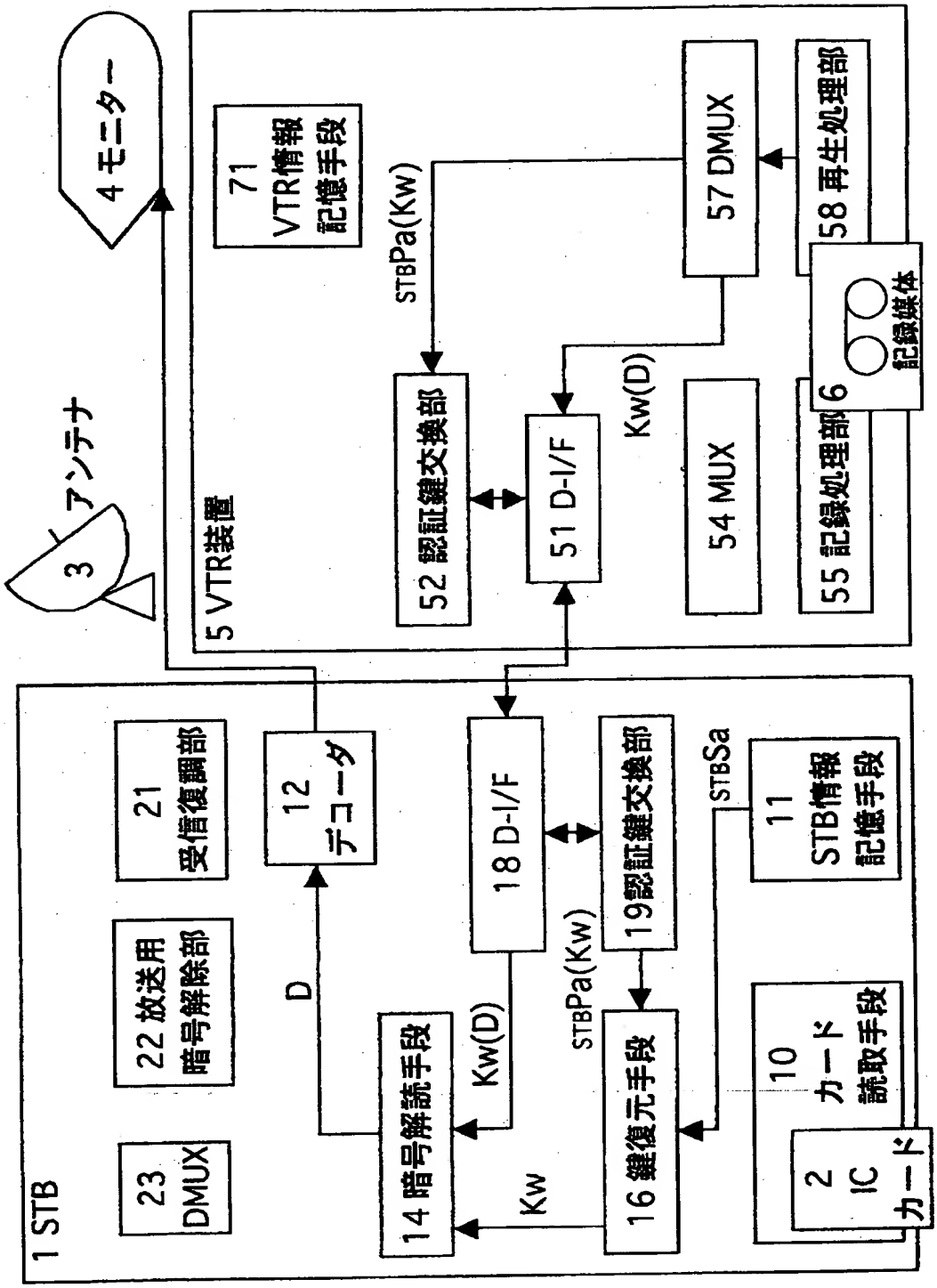
【図１０】


4 モニター
3 アンテナ
5 VTR装置
71 VTR情報記憶手段
61 鍵復元手段
62 鍵暗号化手段
50 STB伝達手段
52 認証鍵交換部
51 D-I/F
56 再生手段
57 DMUX
58 再生処理部
53 記録手段
54 MUX
55 記録処理部
6 記録媒体
1 STB
20 受信手段
21 受信復調部
22 放送用暗号解除部
23 DMUX
12 デコーダ
17 VTR伝達手段
18 D-I/F
19 認証鍵交換部
11 STB情報記憶手段
13 暗号化手段
14 暗号解読手段
31 鍵暗号化手段
16 鍵復元手段
10 カード読取手段
2 IC カード

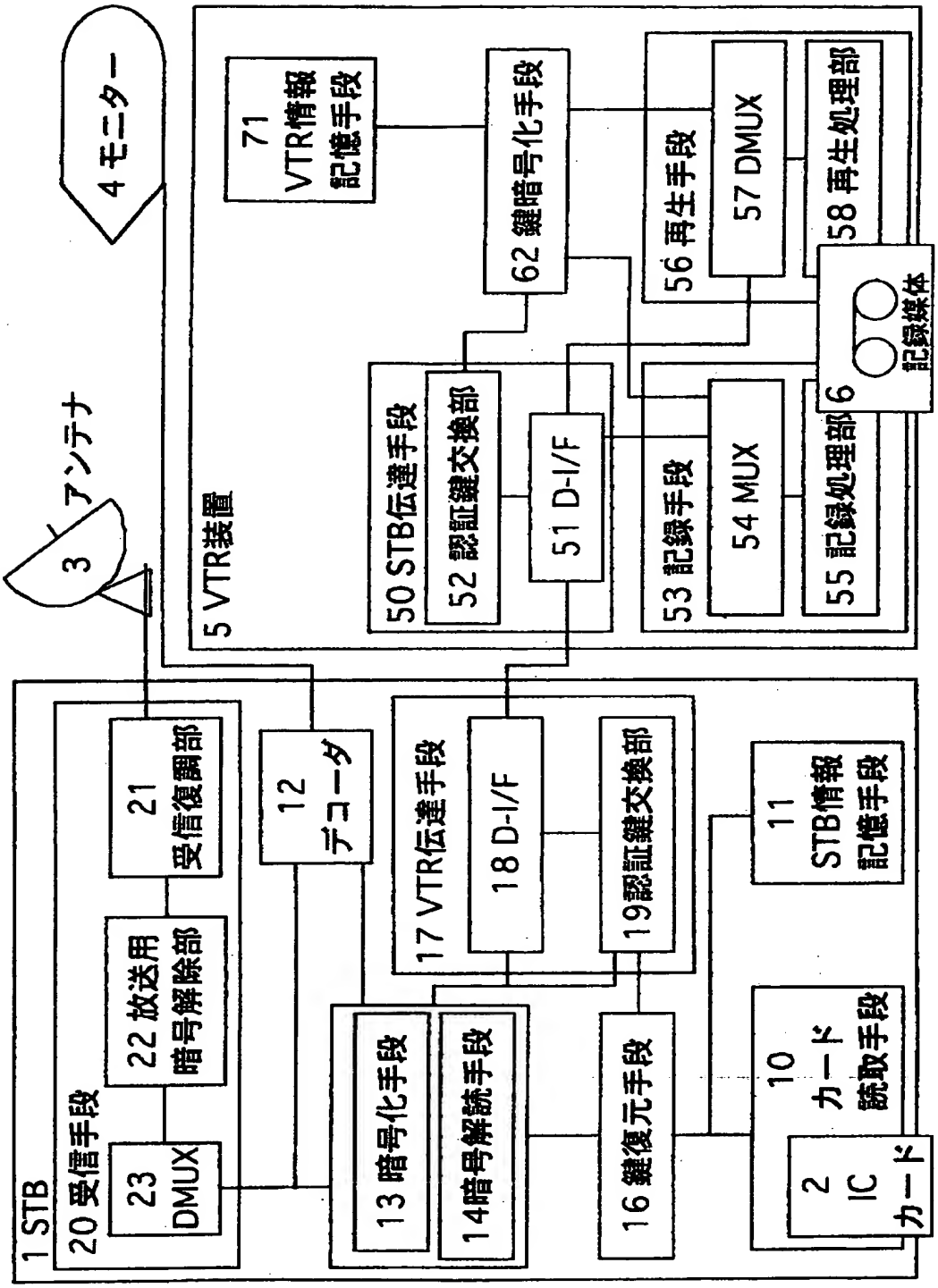
【図１１】


4 モニター
3 アンテナ
5 VTR装置
71 VTR情報記憶手段
STBPa
62 鍵暗号化手段
57 DMUX
58 再生処理部
Kc
Kw
61 鍵復元手段
52 認証鍵交換部
51 D-I/F
STBPa(Kw)
54 MUX
55 記録処理部
6 記録媒体
Kc(Kw)
Kw(D)
1 STB
21 受信復調部
12 デコーダ
18 D-I/F
19認証鍵交換部
11 STB情報記憶手段
22 放送用暗号解除部
23 DMUX
D
13 暗号化手段
Kw(D)
Kc(Kw)
Kc
10 カード読取手段
Kw
31 鍵暗号化手段
2 IC カード

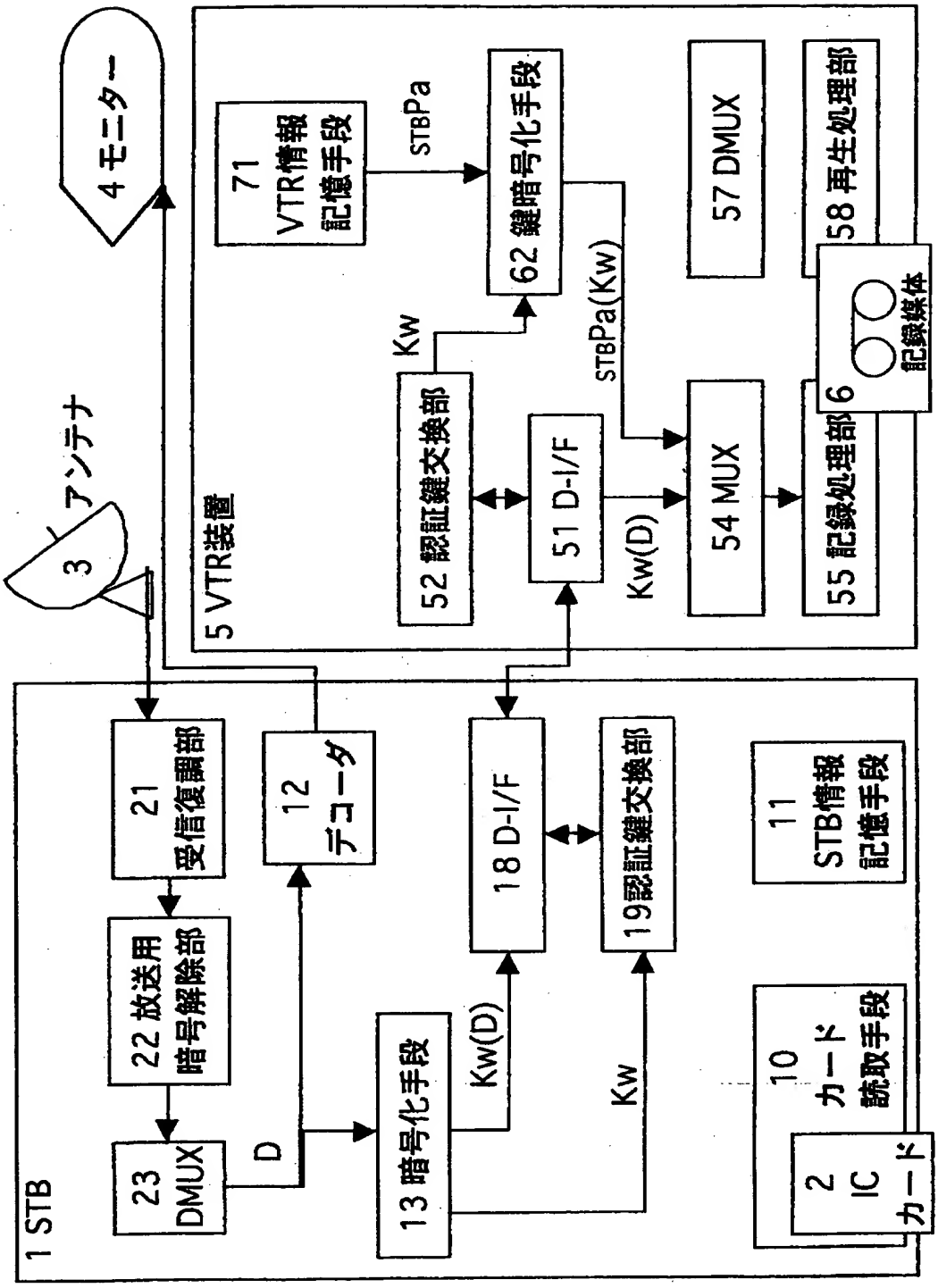
【図１２】


4 モニター
3 アンテナ
5 VTR装置
71 VTR情報記憶手段
STBPa(Kw)
57 DMUX
58 再生処理部
記録媒体
6
52 認証鍵交換部
51 D-I/F
Kw(D)
54 MUX
55 記録処理部
1 STB
21 受信復調部
12 デコーダ
18 D-I/F
19認証鍵交換部
STBSa
11 STB情報記憶手段
22 放送用暗号解除部
D
Kw(D)
STBPa(Kw)
14 暗号解読手段
16 鍵復元手段
10 カード読取手段
23 DMUX
Kw
2 IC カード

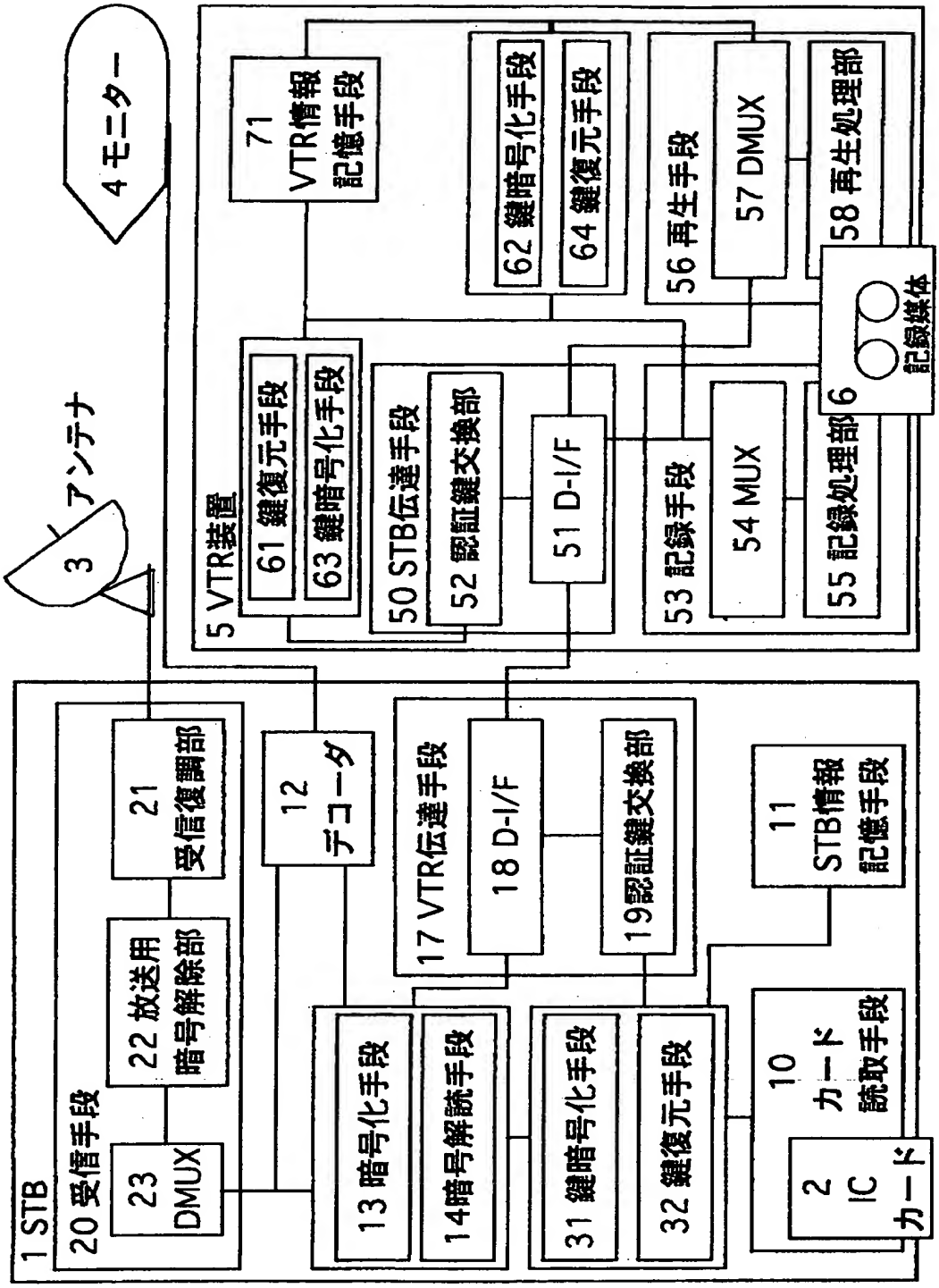
【図１３】


4 モニター
3 アンテナ
1 STB
20 受信手段
21 受信復調部
22 放送用 暗号解除部
23 DMUX
12 デコーダ
13 暗号化手段
14暗号解読手段
17 VTR伝達手段
18 D-I/F
19認証鍵交換部
16 鍵復元手段
11 STB情報 記憶手段
10 カード 読取手段
2 IC カード
5 VTR装置
71 VTR情報 記憶手段
62 鍵暗号化手段
50 STB伝達手段
52 認証鍵交換部
51 D-I/F
56 再生手段
57 DMUX
58 再生処理部
53 記録手段
54 MUX
55 記録処理部
6 記録媒体

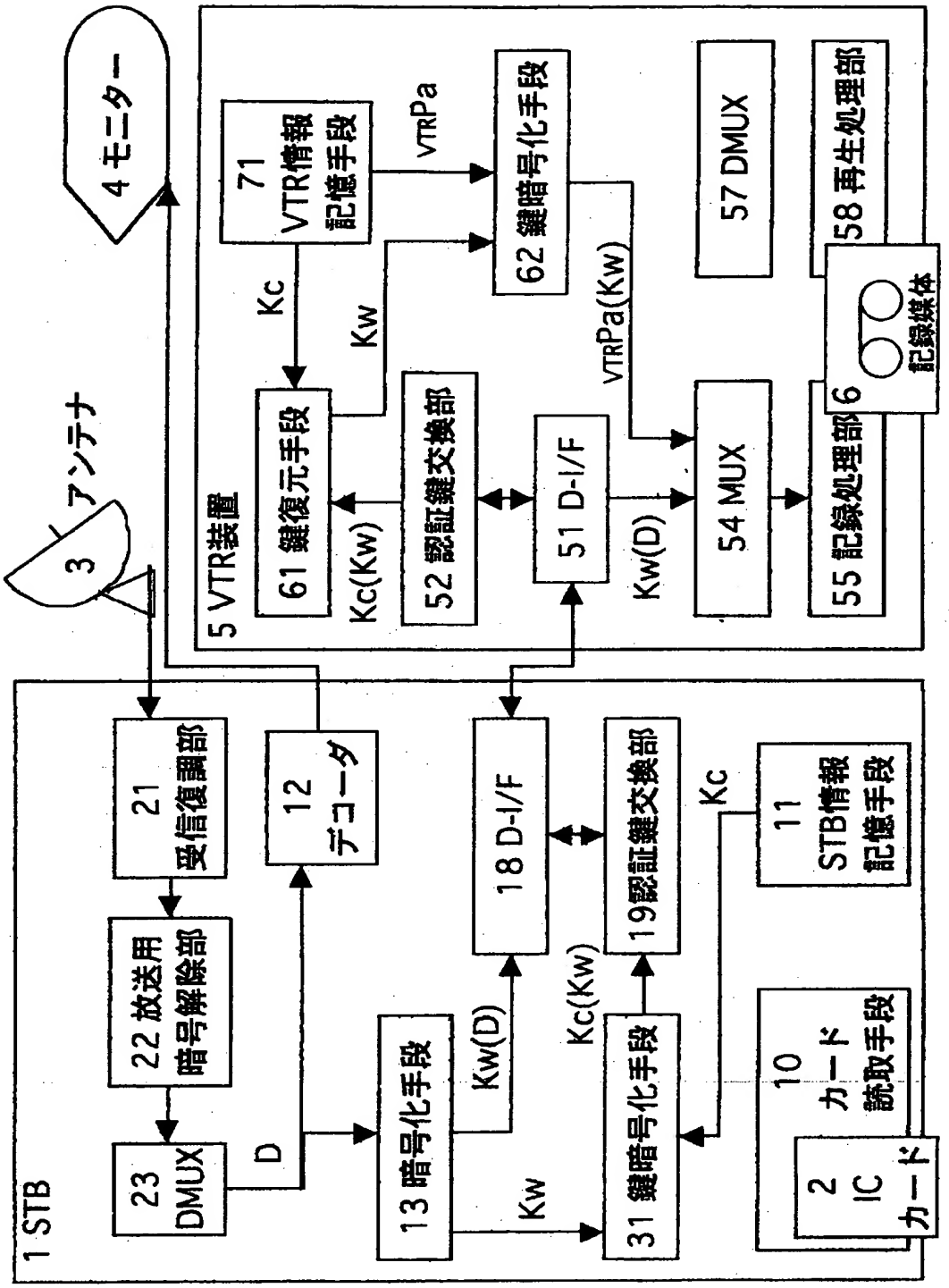
【図１４】


4 モニター
3 アンテナ
5 VTR装置
71 VTR情報記憶手段
STBPa
62 鍵暗号化手段
57 DMUX
58 再生処理部
Kw
STBPa(Kw)
52 認証鍵交換部
51 D-I/F
54 MUX
55 記録処理部
6 記録媒体
Kw(D)
1 STB
21 受信復調部
12 デコーダ
18 D-I/F
19認証鍵交換部
11 STB情報記憶手段
22 放送用暗号解除部
13 暗号化手段
Kw(D)
Kw
10 カード読取手段
23 DMUX
D
2 IC カード

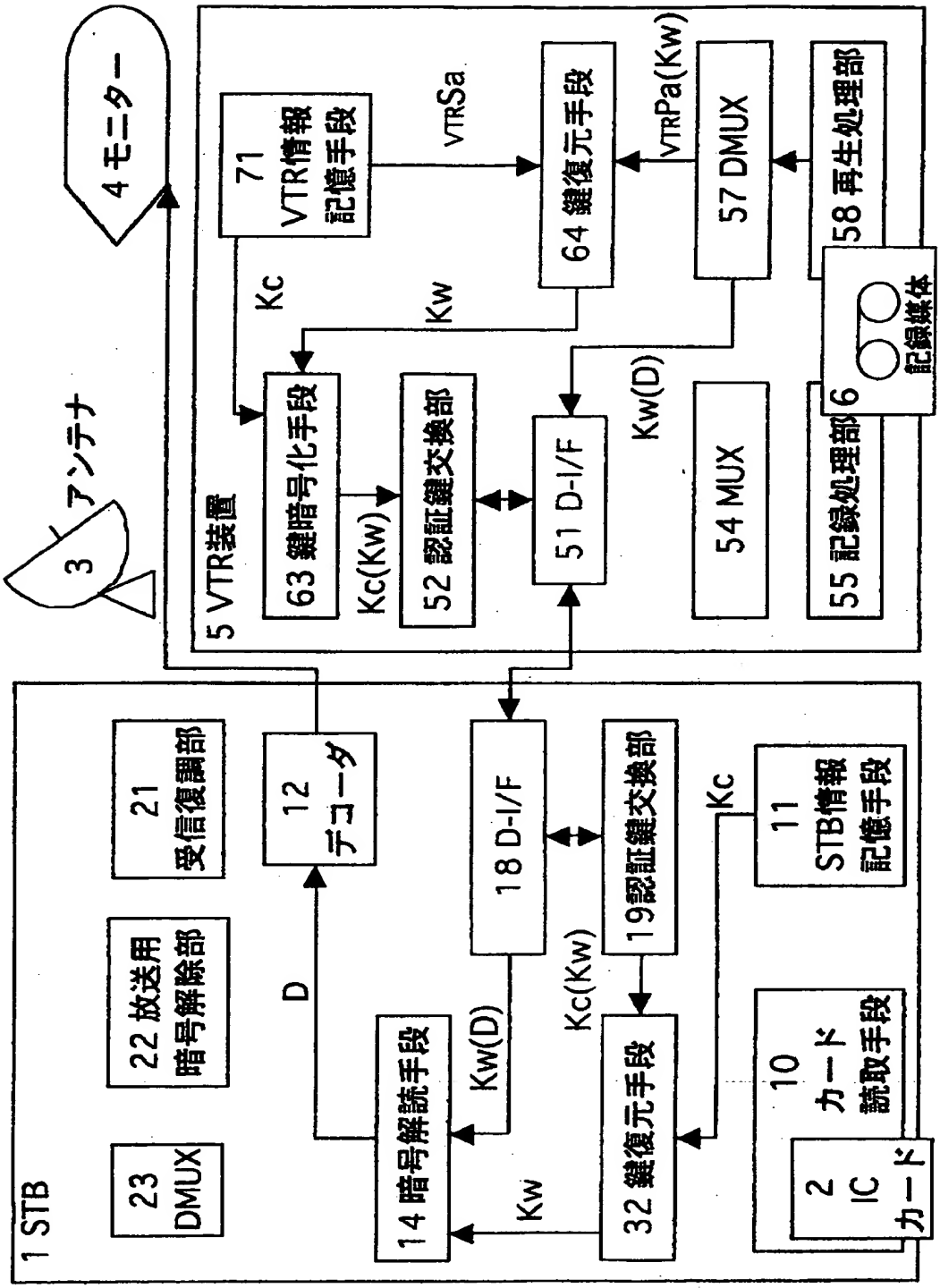
【図１５】


4 モニター
3 アンテナ
71 VTR情報 記憶手段
62 鍵暗号化手段
64 鍵復元手段
56 再生手段
57 DMUX
58 再生処理部
5 VTR装置
61 鍵復元手段
63 鍵暗号化手段
50 STB伝達手段
52 認証鍵交換部
51 D-I/F
53 記録手段
54 MUX
55 記録処理部
6 記録媒体
1 STB
20 受信手段
21 受信復調部
22 放送用 暗号解除部
23 DMUX
12 デコーダ
17 VTR伝達手段
18 D-I/F
19認証鍵交換部
11 STB情報 記憶手段
13 暗号化手段
14暗号解読手段
31 鍵暗号化手段
32 鍵復元手段
10 カード 読取手段
2 IC カード

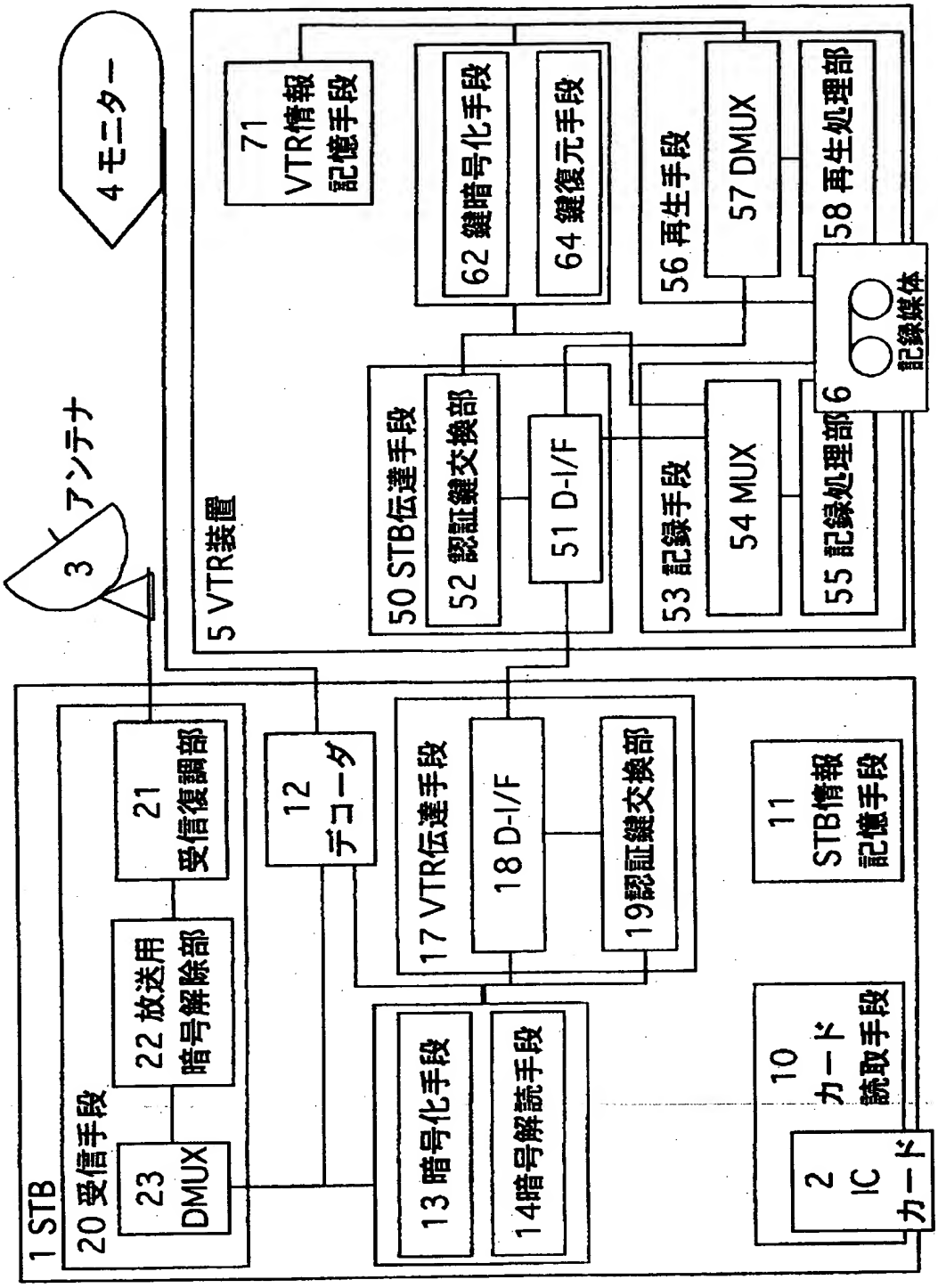
【図１６】


4 モニター
3 アンテナ
5 VTR装置
71 VTR情報記憶手段
VTRPa
62 鍵暗号化手段
57 DMUX
58 再生処理部
Kc
Kw
VTRPa(Kw)
61 鍵復元手段
52 認証鍵交換部
51 D-I/F
54 MUX
55 記録処理部
6 記録媒体
Kc(Kw)
Kw(D)
1 STB
21 受信復調部
12 デコーダ
18 D-I/F
19認証鍵交換部
11 STB情報記憶手段
22 放送用暗号解除部
13 暗号化手段
Kw(D)
Kc(Kw)
Kc
23 DMUX
D
Kw
31 鍵暗号化手段
10 カード読取手段
2 IC カード

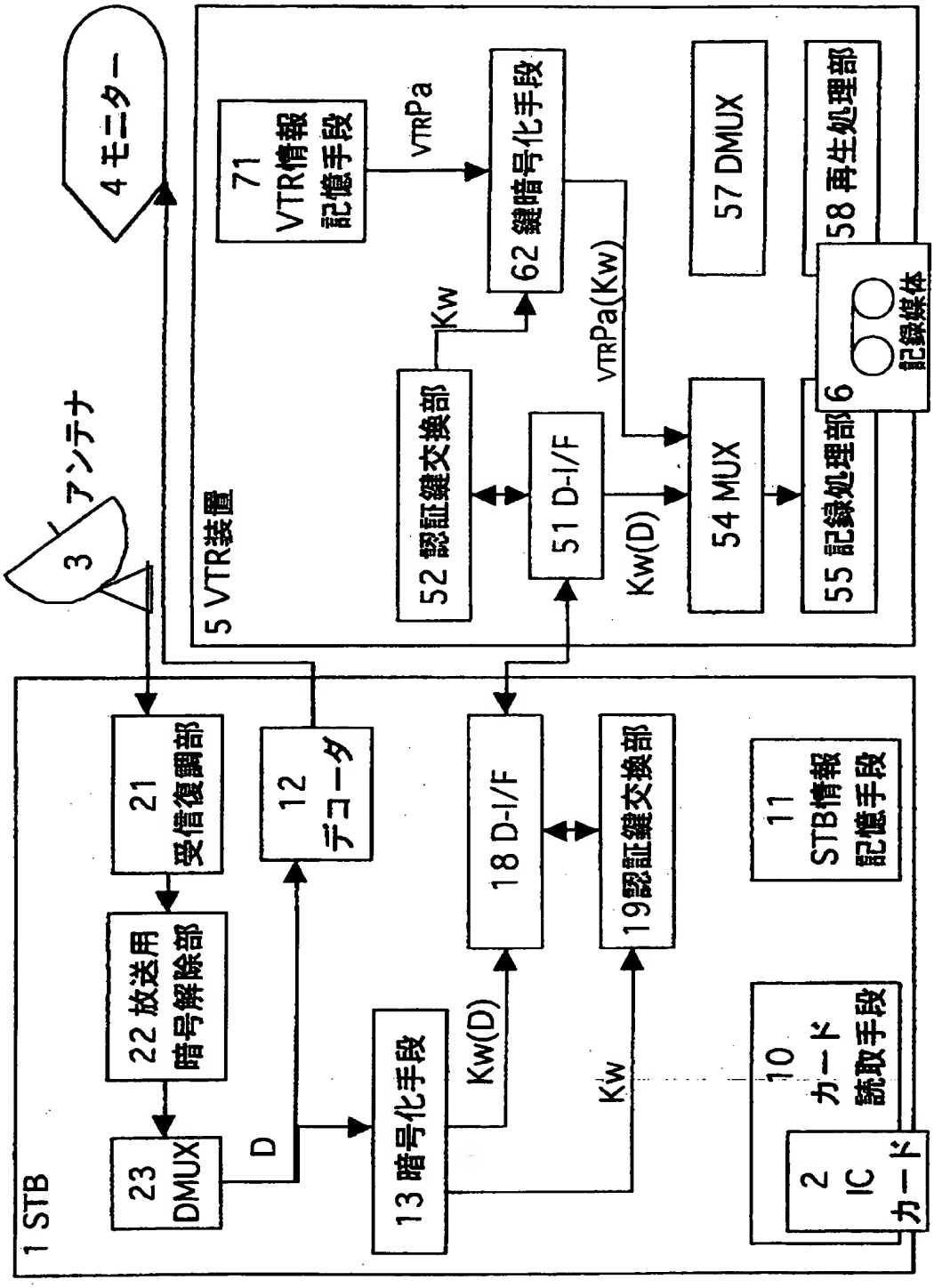
【図１７】


4 モニター
3 アンテナ
5 VTR装置
71 VTR情報記憶手段
VTRSa
64 鍵復元手段
VTRPa(Kw)
57 DMUX
58 再生処理部
Kc
Kw
63 鍵暗号化手段
Kc(Kw)
52 認証鍵交換部
51 D-I/F
Kw(D)
54 MUX
55 記録処理部
6 記録媒体
1 STB
21 受信復調部
12 デコーダ
18 D-I/F
19認証鍵交換部
11 STB情報記憶手段
22 放送用暗号解除部
D
Kw(D)
Kc(Kw)
Kc
23 DMUX
14 暗号解読手段
32 鍵復元手段
10 カード読取手段
Kw
2 IC カード

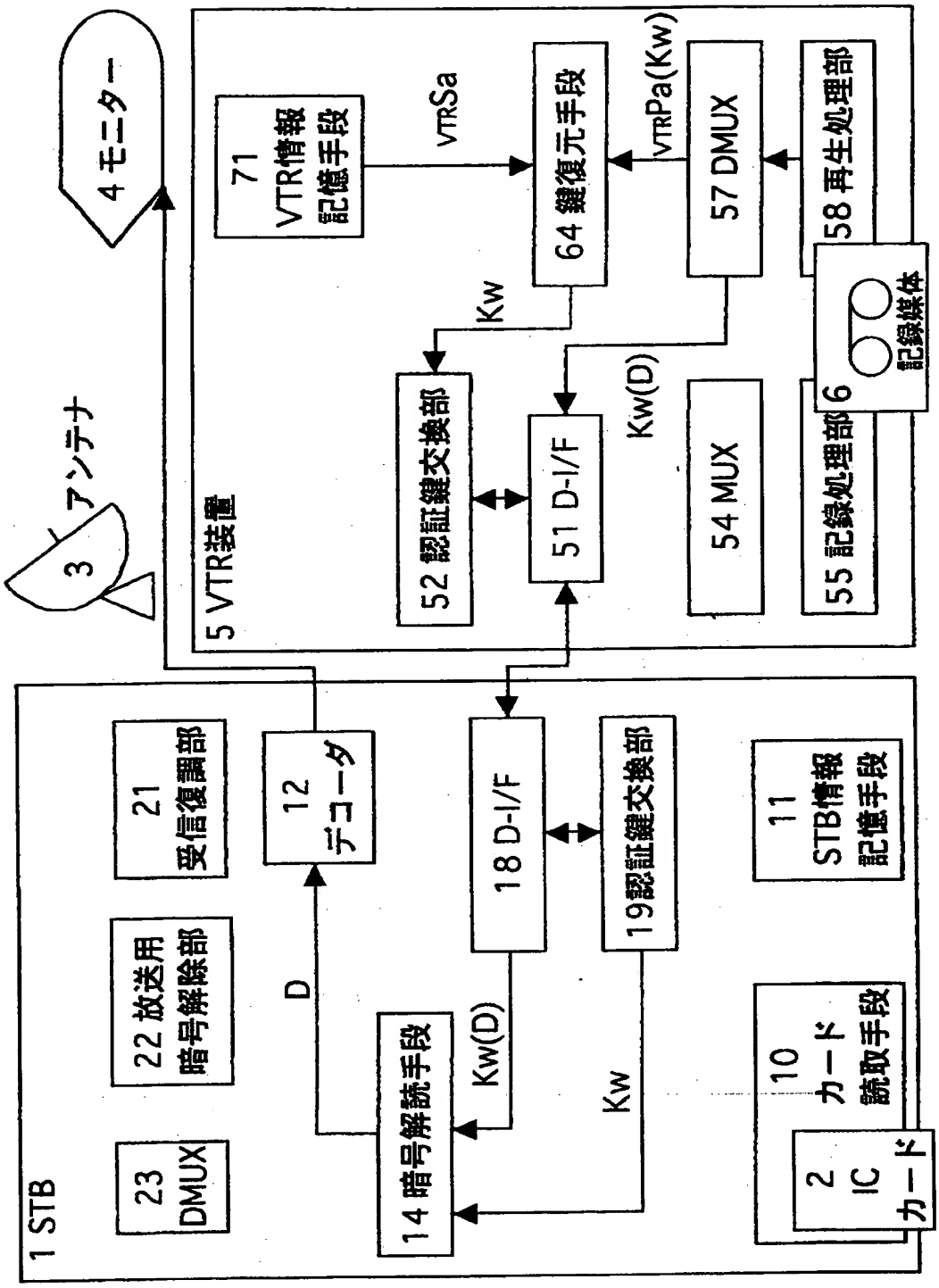
【図１８】


4 モニター
3 アンテナ
5 VTR装置
71 VTR情報記憶手段
62 鍵暗号化手段
64 鍵復元手段
56 再生手段
57 DMUX
58 再生処理部
記録媒体
6
50 STB伝達手段
52 認証鍵交換部
51 D-I/F
53 記録手段
54 MUX
55 記録処理部
1 STB
20 受信手段
21 受信復調部
22 放送用 暗号解除部
23 DMUX
12 デコーダ
17 VTR伝達手段
18 D-I/F
19認証鍵交換部
11 STB情報 記憶手段
13 暗号化手段
14暗号解読手段
10 カード 読取手段
2 IC カード

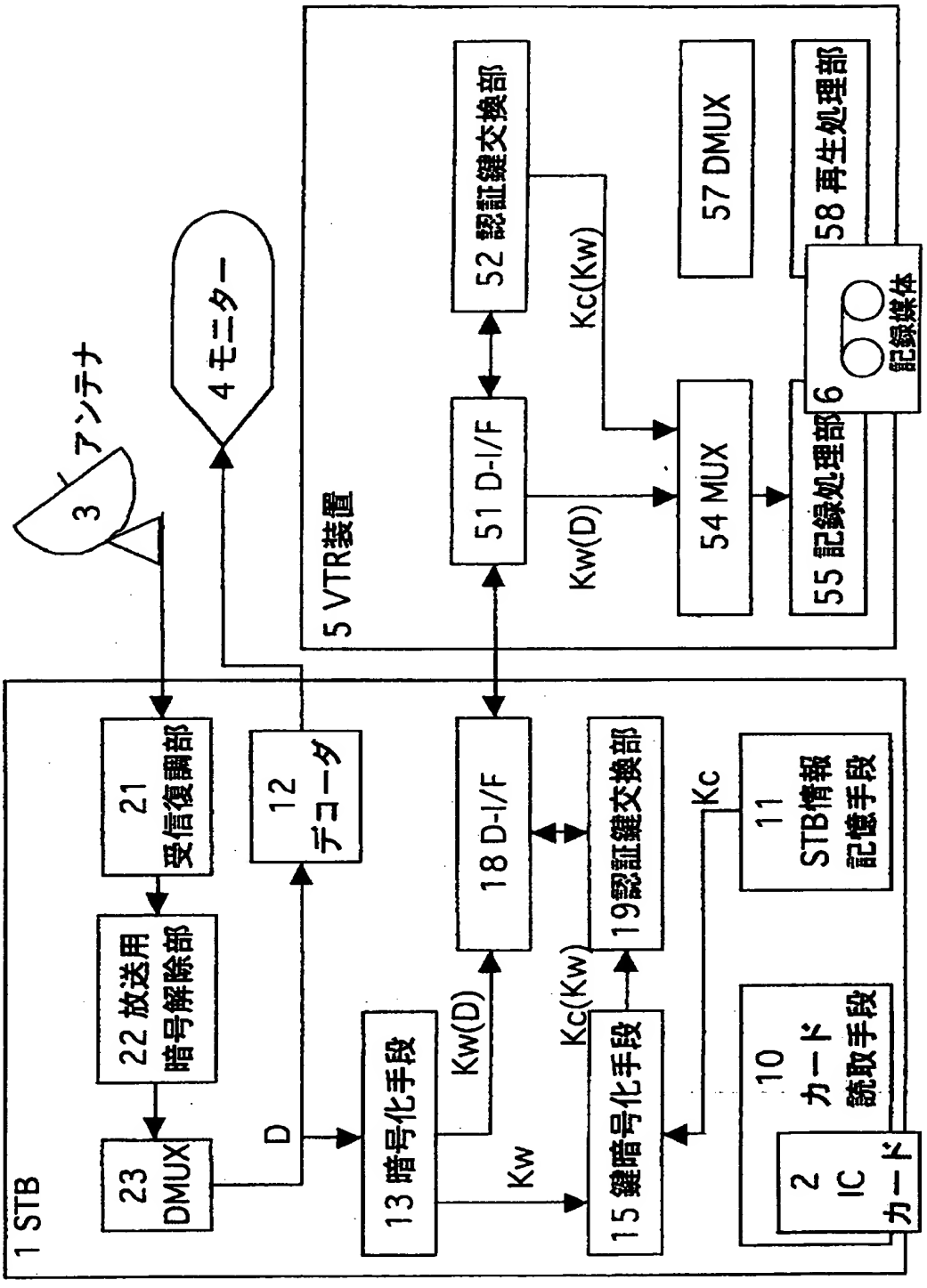
【図１９】


4 モニター
3 アンテナ
5 VTR装置
71 VTR情報記憶手段
VTRPa
62 鍵暗号化手段
57 DMUX
58 再生処理部
Kw
VTRPa(Kw)
6 記録媒体
52 認証鍵交換部
51 D-I/F
Kw(D)
54 MUX
55 記録処理部
1 STB
21 受信復調部
12 デコーダ
18 D-I/F
19 認証鍵交換部
11 STB情報記憶手段
22 放送用暗号解除部
23 DMUX
D
13 暗号化手段
Kw(D)
Kw
10 カード読取手段
2 IC カード

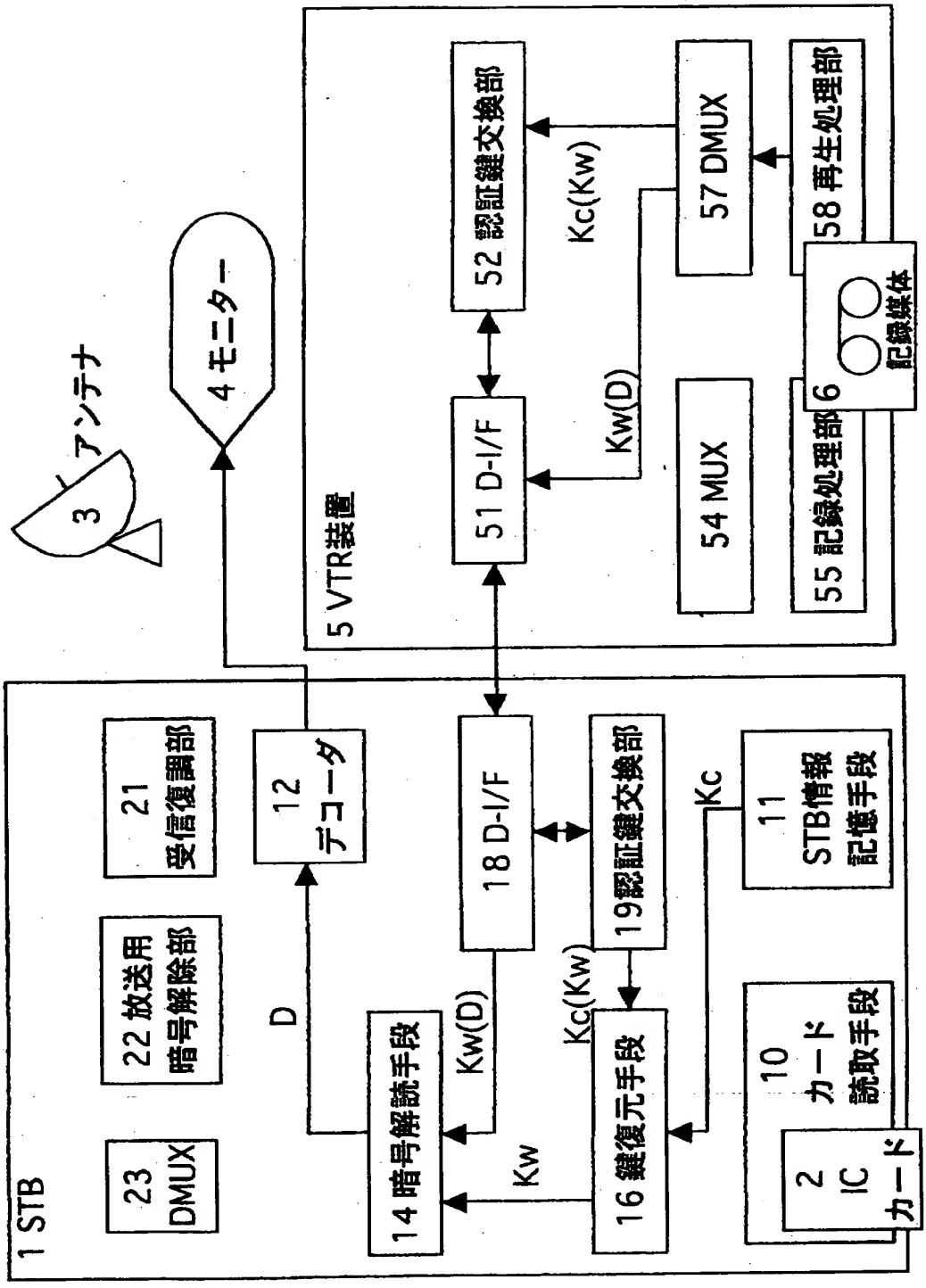
【図２０】


4 モニター
3 アンテナ
5 VTR装置
71 VTR情報記憶手段
VTRSa
64 鍵復元手段
VTRPa(Kw)
57 DMUX
58 再生処理部
Kw
52 認証鍵交換部
51 D-I/F
Kw(D)
54 MUX
55 記録処理部
6 記録媒体
1 STB
21 受信復調部
12 デコーダ
18 D-I/F
19 認証鍵交換部
11 STB情報記憶手段
22 放送用暗号解除部
D
Kw(D)
14 暗号解読手段
Kw
10 カード読取手段
23 DMUX
2 IC カード

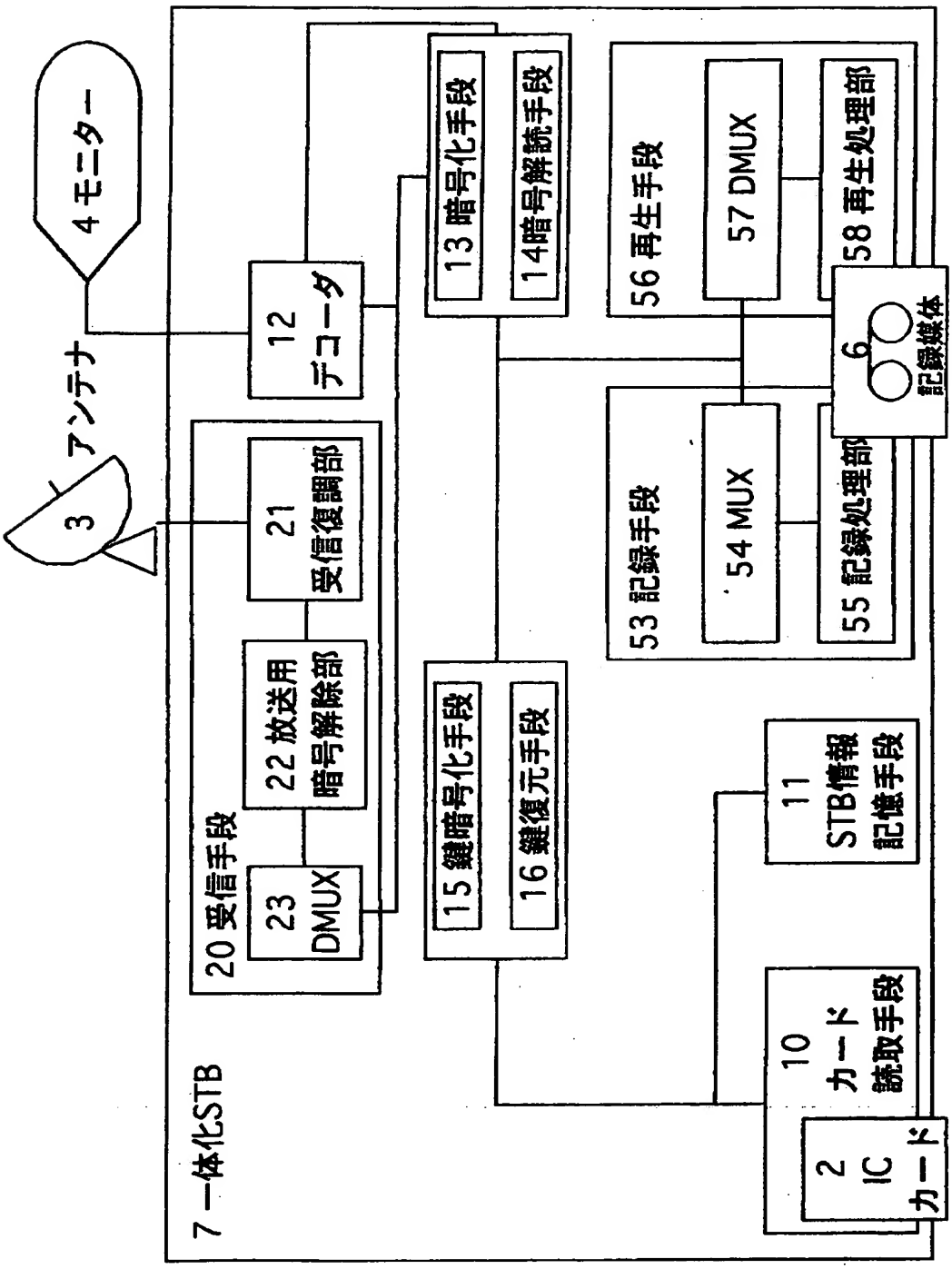
【図２１】


1 STB
2 IC カード
3 アンテナ
4 モニター
5 VTR装置
6 記録媒体
10 カード読取手段
11 STB情報記憶手段
12 デコーダ
13 暗号化手段
15 鍵暗号化手段
18 D-I/F
19 認証鍵交換部
21 受信復調部
22 放送用暗号解除部
23 DMUX
51 D-I/F
52 認証鍵交換部
54 MUX
55 記録処理部
57 DMUX
58 再生処理部
D
Kw
Kw(D)
Kc(Kw)
Kc

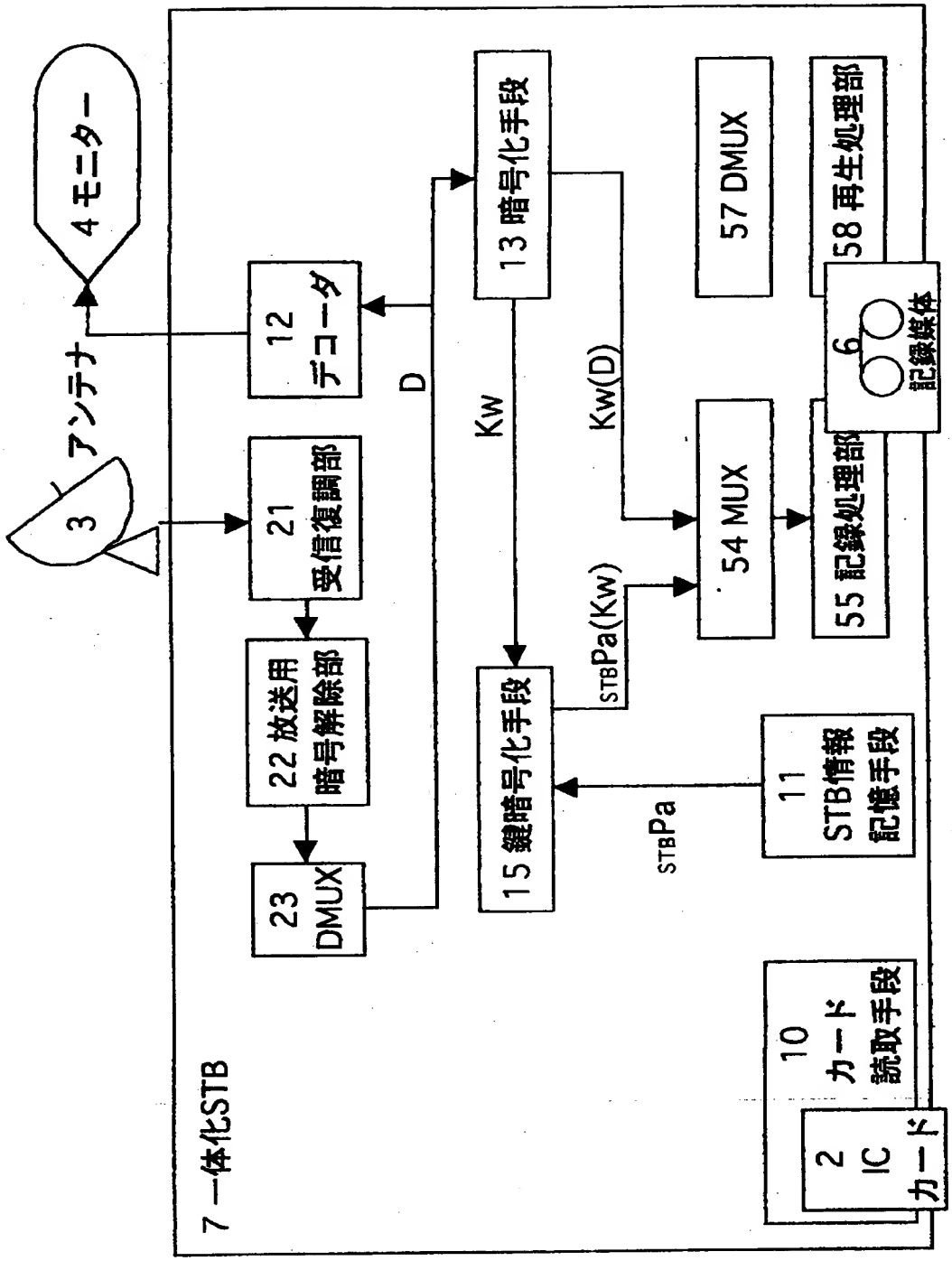
【図２２】


1 STB
2 IC カード
10 カード読取手段
11 STB情報記憶手段
12 デコーダ
14 暗号解読手段
16 鍵復元手段
18 D-I/F
19認証鍵交換部
21 受信復調部
22 放送用暗号解除部
23 DMUX
3 アンテナ
4 モニター
5 VTR装置
51 D-I/F
52 認証鍵交換部
54 MUX
55 記録処理部
57 DMUX
58 再生処理部
6 記録媒体
D
Kw
Kw(D)
Kc(Kw)
Kc

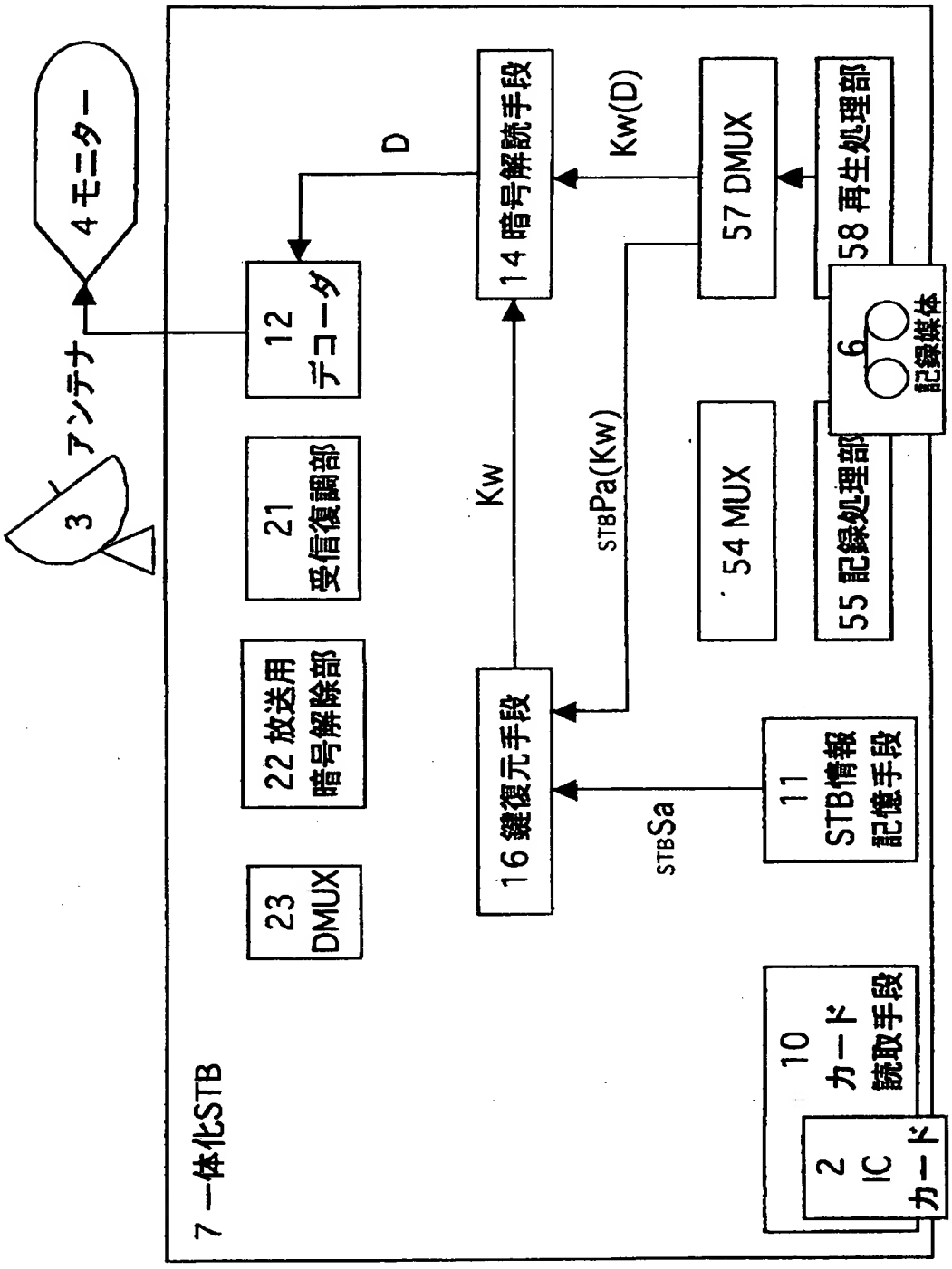
【図２３】


4モニター
3 アンテナ
12 デコーダ
13 暗号化手段
14暗号解読手段
56 再生手段
57 DMUX
58 再生処理部
6 記録媒体
21 受信復調部
22 放送用 暗号解除部
23 DMUX
20 受信手段
15 鍵暗号化手段
16 鍵復元手段
53 記録手段
54 MUX
55 記録処理部
11 STB情報 記憶手段
10 カード 読取手段
2 IC カード
7 一体化STB

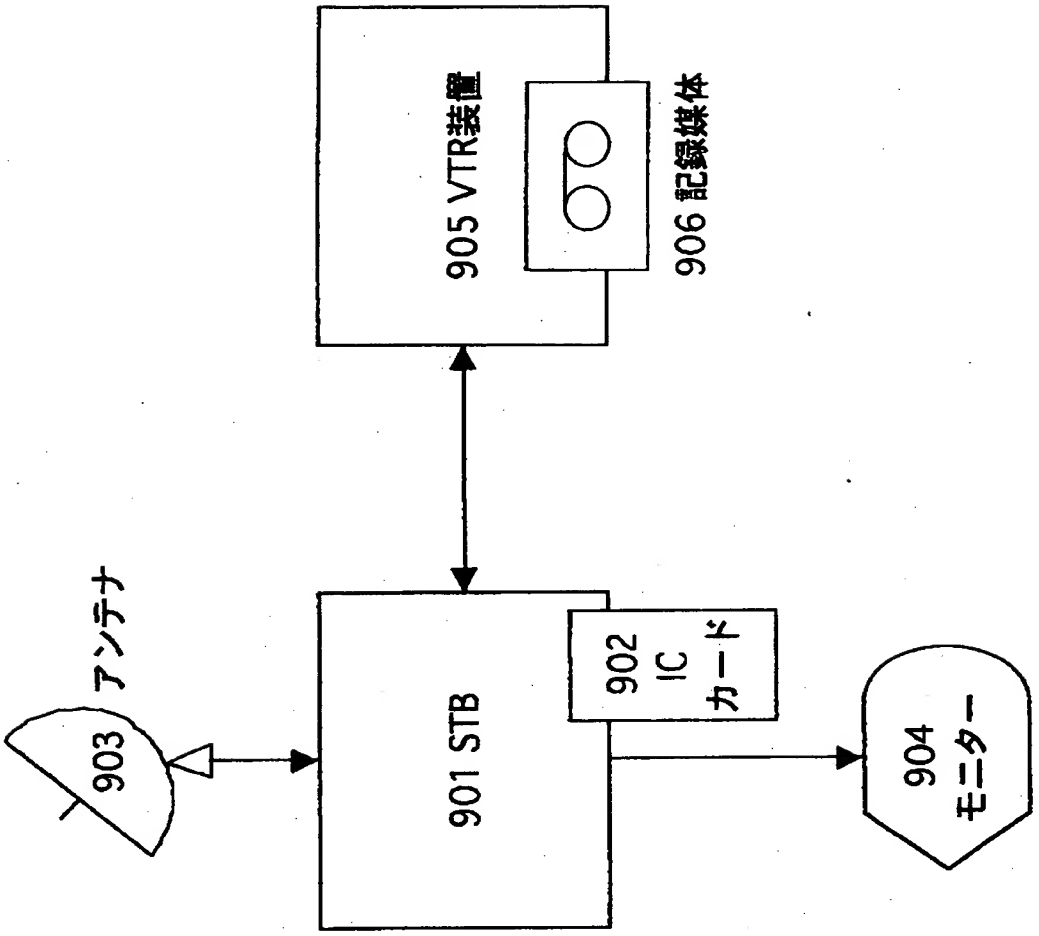
【図２４】


4 モニター
アンテナ
3
12 デコーダ
21 受信復調部
22 放送用 暗号解除部
23 DMUX
D
13 暗号化手段
Kw
15 鍵暗号化手段
STBPa(Kw)
STBPa
11 STB情報 記憶手段
Kw(D)
57 DMUX
54 MUX
58 再生処理部
55 記録処理部
6 記録媒体
10 カード 読取手段
2 IC カード
7 一体化STB

【図２５】


4 モニター
アンテナ
3
12 デコーダ
21 受信復調部
22 放送用 暗号解除部
23 DMUX
D
14 暗号解読手段
Kw(D)
57 DMUX
58 再生処理部
6 記録媒体
Kw
STBPa(Kw)
54 MUX
55 記録処理部
16 鍵復元手段
STBSa
11 STB情報 記憶手段
10 カード 読取手段
2 IC カード
7 一体化STB

【図２６】



【書類名】要約書

【要約】

【課題】　特定の対象に対してのみ、再生が可能であり、前記暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムを提供する。

【解決手段】　ディジタルデータを受信する受信手段２０と、ワークキーを生成し、前記ディジタルデータに前記ワークキーを用いて暗号化を施して暗号化ディジタルデータを生成する暗号化手段１３と、前記ワークキーに第２の暗号化を施して暗号化ワークキーを生成する鍵暗号化手段１５と、前記暗号化ディジタルデータおよび前記暗号化ワークキーを記録媒体６に記録する記録手段５３と、記録媒体６から前記暗号化ディジタルデータおよび前記暗号化ワークキーを再生する再生手段５６と、前記暗号化ワークキーを解読して前記ワークキーを復元する鍵復元手段１６と、復元された前記ワークキーを用いて前記暗号化ディジタルデータを解読して、前記ディジタルデータを得る暗号解読手段１４とを備える。

【選択図】　図１

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000005821
【住所又は居所】　大阪府門真市大字門真１００６番地
【氏名又は名称】　松下電器産業株式会社
【代理人】　申請人
【識別番号】　100092794
【住所又は居所】　大阪市淀川区宮原５丁目１番３号　新大阪生島ビル　松田特許事務所
【氏名又は名称】　松田　正道

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社

BLANK PAGE